Zoran Šami

PRILOG REŠAVANJU FERMAT-OVOG PROBLEMA

doktorska disertacija

Beograd 1978

U V O D

Snažan impuls teoriji brojeva dao je francuski pravnik i matematičar Pierre de Fermat (1601-1665). Kao amater u matematici, za života nije objavio gotovo ništa od svojih radova, ali je zato pokoljenjima matematičara ostavio u nasledje mnoštvo razradjenih ili nerazradjenih ideja. Mnoge njegove hipoteze su dokazane, neke su oborene, ali jedna i dalje odoleva napadu matematičara i samim tim raspaljuje njihovu maštu. Gotovo da nema matematičara, bio on početnik, kao autor ovog rada, ili veliki priznati naučnik, kao na primer, Euler, koji se s njom nije uhvatio u koštac. Medjutim, Fermat-ovo tvrdjenje: Jednačina

$$x^n + y^n = z^n, \quad n \in N, \ n>2,$$

nema rešenja u skupu prirodnih brojeva, nije ni do danas ni dokazano, ni oboreno. Ovo tvrdjenje, poznato u literaturi pod imenom "Veliki Fermat-ov problem", tema je ovog rada.

Dobar je običaj da se na početku svakog izlaganja da istorijski osvrt na problematiku koju nameravamo da razmatramo. Ovde je situacija specifična utoliko, što bi nabrajanje samo značajnijih rezultata vezanih za Fermat-ov problem, zauzelo mnogo, veoma mnogo prostora. Zadovoljimo se stoga, jednim okvirnim pregledom istorijskih činjenica.

Prvi objavljeni dokaz Fermat-ovog tvrdjenja za $n=3$ dao je 1774 godine Euler. Vrlo je verovatno, da je nezavisno od opšteg slučaja, Fermat imao u vidu ovaj dokaz. Euler-ov dokaz nije bio sasvim potpun; nedostaci su otklonjeni kada je Lagrange objavio svoje radove iz teorije binarnih kvadratnih formi. Dokaz Fermat-ovog tvrdjenja za $n=5$ dali su Legendre i Dirichlet, za $n=7$ Lamé. Ozbiljniji pohod na opšti slučaj Fermat-ovog problema načinio je Kummer, čija se ideja da izadje iz okvira elementarne

teorije brojeva i zagazi duboko u teoriju algebarskih struktura, pokazala isto toliko efikasnom koliko i elegantnom. Bez obzira na to, što su Kummer-ovi rezultati tokom vremena poboljšavani,oni se ni danas ne mogu da zaobidju u iole ozbiljnijem prikazivanju Fermat-ovog problema. Iz tog razloga, i mi ćemo im u našem izlaganju ukazati dužnu pažnju.

Pogledajmo sad šta je pred nama. Rad je podeljen na četiri glave. U prvoj glavi, koja sadrži osam odeljaka, izlažu se oni rezultati postignuti do sada u rešavanju Fermat-ovog problema, koji su nam se, iz ma kojeg razloga, učinili značajnim.Odeljci 1.1 i 1.2 posvećeni su specijalnim slučajevima $n=2$ i $n=4$.Tu se s jedne strane izvodi opšti oblik rešenja jednačine $x^2+y^2=z^2$, a s druge strane se dokazuje da je za $n=4$ Fermat-ovo tvrdjenje tačno.

Sa odeljkom 1.3 započinjemo tretiranje opšteg slučaja Fermat-ovog problema, razmatrajući neke osnovne činjenice vezane za njega. Tu vrlo brzo zaključujemo da je dovoljno posmatrati slučaj $n=p\in P$,kao i da je praktično razmatrati odvojeno dve mogućnosti: prvu, kad je $xyz\not\equiv o \pmod p$,tzv. prvi slučaj Fermat-ovog problema, i drugu, kad je $xyz\equiv o \pmod p$, tzv. drugi slučaj Fermat-ovog problema. Dalje se dokazuju neka osnovna tvrdjenja vezana za Fermat-ov problem. To su, u stvari, prvi rezultati autora ovog rada iz vremena kada je počinjao da se bavi Fermat-ovim problemom. Naravno, kao što se početnicima često dogadja, ti rezultati su poznati odavno. Tako je leme 1.3 i 1.4 dokazao Barlow(kao i Abel), lemu 1.5 Euler, lemu 1.6 Vandiver (mada, istini za volju, njegov dokaz nije bio elementaran).

U odeljcima 1.4 i 1.5 privremeno napuštamo Fermat-ov problem, da bi se naoružali dovoljnim brojem pojmova i stavova iz Više algebre. Tako u odeljku 1.4 definišemo algebarske brojeve, kao i osnovne pojmove vezane za njih. Zatim razmatramo jednotne elemente u integralnom domenu kao i problem faktorizacije. Izlažemo zatim ideju primene tih algebarskih struktura na teoriju brojeva, i uočavamo, da je jedna od glavnih smetnji efikasnosti te primene problem jednoznačne faktorizacije. Da bismo rešili taj problem uvodimo teoriju divizora. U odeljku 1.5 navodimo i dokazujemo nekoliko lema vezanih za pojmove uvedene u prethodnom odeljku, koje kasnije direktno koristimo.

Odeljak 1.6 posvećen je ranije pomenutom Kummer-ovom rezultatu. Tu formulišemo i dokazujemo Kummer-ovu teoremu da je Fermat-ovo tvrdjenje tačno za sve proste regularne brojeve p. Rad Kummer-a prisutan je i u sledećem, sedmom odeljku. Tu se,naime, navode najznačajniji rezultati postignuti u razmatranju prvog slučaja Fermat-ovog problema, a ti rezultati su, uglavnom, posledice tzv. Kummer-ove leme. Ta lema, koju mi navodimo kao teoremu 1.14, biće koren nekih originalnih rezultata autora ovog rada, koji će biti izneti u četvrtoj glavi.

Konačno, u odeljku 1.8 bavimo se Bernoulli-jevim brojevima, koji na više mesta u ovom radu igraju značajnu ulogu.Pored definicije, tu se dokazuju neki manje-više poznati stavovi vezani za njih.

Originalni rezultati autora smešteni su u preostale tri glave rada. Druga glava predstavlja generalizaciju rezultata do kojih je autor došao u [51]. Naime, u [51] (38-41) dokazana je teorema: Ako je bar jedan od brojeva $2p+1$, $4p+1$ prost, tada jednačina

$$x^p + y^p = z^p, \quad x,y,z \in N, \quad p \in P, \quad p \geq 3$$

nema rešenja relativno prosta sa p. Sav naš trud u drugoj glavi biće da dokažemo, da u iskazu gornje teoreme može umesto "$2p+1$, $4p+1$" da stoji "$2^m np+1$, $m \in N$, $n=1$ ili $n \in P$, $n \geq 5$",uz ispunjenje još nekih dodatnih uslova, datih u obliku pogodnom za proveru.

U tom cilju, u odeljku 2.1 dokazuje se direktna veza izmedju prvog slučaja Fermat-ovog problema i problema da li par kongruencija

$$t^s \equiv 1, \quad (t+1)^s \equiv 1 \pmod{q}, \quad q=sp+1 \in P$$

ima zajednička rešenja. Na taj način naša dalja pažnja biće usmerena na uočeni par kongruencija.

U odeljku 2.2 definišemo izvestan broj cikličkih determinanti. Zatim pokazujemo da se takve determinante mogu svesti na konačne proizvode trigonometrijskih funkcija,što čini njihovo izračunavanje veoma efikasnim. Koristeći rezultate ovog odeljka u narednom, trećem odeljku rešavamo postavljeni problem o paru kongruencija za slučaj $s=2^m n$, $m \in N$, $n \in P$, $n \geq 5$ ili $n=1$.

Konačno, u odeljku 2.4 stižemo do cilja, dokazujući napred navedenu teoremu o prvom slučaju Fermat-ovog problema.

ći više, teoremama 2.4 i 2.5 pokazujemo da se dokazana teorema (teorema 2.3) može vrlo dobro poboljšati. Druga metoda, pokazuje o da se je tavljeni u lovi a teoremi 2.3 mogu vrlo jednostavno proveriti.

Treća glava predstavlja celina sama za sebe. U njoj se mi nigde ne dotičemo Fermat-ovog problema, mada, što se može i očekivati, činjenice utvrdjene u ovoj glavi biće u četvrtoj glavi veoma dobro primenjene na prvi slučaj Fermat-ovog problema. Konkretno, u odeljku 3.1 definiše se niz brojeva $x_{n,k}$ i dokazuju se neke njegove interesantne osobine. U 3.2 se, koristeći vezu izmedju $x_{n,k}$ i funkcije $!n = 1+1!+2!+\ldots+(n-1)!$, izvodi jedna interesantna formula za $!n$, na osnovu koje se opet, izvodi hipoteza ekvivalentna hipotezi Dj.Kurepe da je $(!n,n!)=2$ za svako $n \in N$, $n \geq 2$.

Odeljci 3.3 i 3.4 posvećeni su nizu polinoma $D_k(x)$ $(k-1)$-og stepena, kojeg definišemo u 3.3. Tu se dokazuje niz interesantnih osobina ovog niza polinoma, pre svega, njegova organska veza sa nizom $x_{n,k}$. Izmedju ostalog, dokazuje se da je $D_k(1)=1$ za svako $k \in N$, $D_k(2)=0 \Leftrightarrow k$ je parno , $D_k(x) = (1-x)^{k-1} D_k(\frac{x}{x-1})$, $x \neq 1$, i tome slično.

Kao što rekosmo, četvrta glava predstavlja primenu rezultata treće glave, konkretno niza $D_k(x)$, na prvi slučaj Fermat-ovog problema. Osnov te primene iznet je u odeljku 4.1, u kojem dokazujemo teoremu 4.1 ekvivalentnu Kummer-ovoj lemi (teorema 1.14) iznetoj u odeljku 1.7. U odeljku 4.2 primenjujemo dokazanu teoremu 4.1 da bi poboljšali rezultate Cauchy-ja, Kummer-a, Mirimanoff-a i Krasner-a vezane za prvi slučaj Fermat-ovog problema, dokazujući da ako postoji k, $k = 2,4,\ldots,2k_o$, $k_o = max(6, [\frac{1}{2}(1 + \sqrt[5]{ln^2 p})])$, tako da je

$$B_{p-k-1} \not\equiv 0 \pmod{p},$$

gde je B_{p-k-1} Bernoulli-jev broj, tada jednačina

$$x^p + y^p = z^p, \quad x,y,z \in N, \ p \in P, \ p \geq 3,$$

nema rešenja relativno prosta sa p.

U odeljku 4.3 dajemo još jednu primenu niza polinoma $D_k(x)$ na prvi slučaj Fermat-ovog problema, dokazujući poznati

Wieferichov rezultat da je Fermat-ovo tvrdjenje u prvom slučaju tačno, ako je

$$2^{p-1} \not\equiv 1 \pmod{p^2}.$$

U odeljku 4.4 dokazujemo jednu interesantnu vezu između Bernoulli-jevih brojeva i niza polinoma $D_p(x)$. Ta veza nam, između ostalog, omogućuje da uslove izražene teoremama 4.3 i 4.4 stopimo u jedan jedini uslov. Konačno, pokušavajući da damo neki rezime, odeljkom 4.5 zaključujemo naše izlaganje.

Sada nam ne preostaje ništa drugo, nego da po utvrdjenom redosledu počnemo sa izlaganjem.

I G L A V A

1.1 Fermat-ov problem za $n=2$

Započećemo razmatranje Fermat-ovog problema sa najjednostavnijim i dobro poznatim slučajem $n=2$. Dakle, razmatramo jednačinu

$$x^2+ y^2= z^2, \tag{1.1}$$

gde su x,y,z prirodni brojevi. Jednačina (1.1) očigledno ima rešenja; na primer, $x=3$, $y=4$, $z=5$. Naš je zadatak da ukažemo na opšti oblik tih rešenja.

Ne umanjujući opštost možemo pretpostaviti da su x,y,z u jednačini (1.1) dva po dva relativno prosti. Stvarno,ako bi bilo $(x,y)=d>1$, sledilo bi $(x,y,z)=d$, pa bi se jednačina (1.1) mogla da skrati sa d^2.

Teorema 1.1 Uzajamno prosti brojevi x,y,z zadovoljavaju jednačinu (1.1) ako i samo ako važi

$$x=2ab,\ y=a^2-b^2,\ z=a^2+b^2, \tag{1.2}$$

gde je $a>b>o$, $(a,b)=1$,a od brojeva a,b jedan je paran, a drugi neparan.

Dokaz. Neka je ispunjeno (1.2). Tada je

$$(2ab)^2+ (a^2- b^2)^2= a^4+ 2a^2b^2+ b^4= (a^2+ b^2)^2.$$

Takodje, iz $a>b>o$ sledi $x,y,z\in N$. Kako su a i b po pretpostavci relativno prosti i uz to jedan paran a drugi neparan, to su y i z neparni, pa je $(x,y)=(x,z)=1$ i $(y,z)=(a^2- b^2,\ a^2+ b^2)=$ $=(2b^2,\ a^2+ b^2)=(b^2,\ a^2+ b^2)=(b^2,\ a^2)=1$. Time je dovoljnost uslova dokazana.

Neka su sad x,y,z relativno prosti brojevi koji zadovoljavaju jednačinu (1.1). Dokažimo da tada mora da važi (1.2). Pre svega, jedan od brojeva mora biti paran. Stvarno,ako bi oba

bila neparna, sledilo bi

$$z^2 = x^2 + y^2 \equiv 2 \pmod 4,$$

što je nemoguće.

Ne umanjujući opštost možemo pretpostaviti da je x paran. No, onda se jednačina (1.1) može napisati u obliku

$$(\frac{x}{2})^2 = \frac{z+y}{2}\ \frac{z-y}{2}\ , \tag{1.3}$$

pri čemu su $\frac{z+y}{2}$ i $\frac{z-y}{2}$ očigledno relativno prosti. Kako je proizvod dva relativno prosta broja potpun kvadrat prirodnog broja jedino kada je svaki od njih potpun kvadrat, to mora biti

$$\frac{z+y}{2} = a^2, \quad \frac{z-y}{2} = b^2, \quad (a,b)=1, \quad a>b>o. \tag{1.4}$$

Iz (1.3) i (1.4) direktno sledi (1.2). Time je teorema u potpunosti dokazana.

Očigledno, teorema 1.1 daje odgovor na pitanje kako izgleda opšti oblik rešenja jednačine (1.1), a samim tim u potpunosti opisuje specijalan slučaj $n=2$ Fermat-ovog problema.

1.2 Fermat-ov problem za $n=4$

Pokazaćemo da je u ovom slučaju Fermat-ovo tvrdjenje bilo tačno, tj. pokazaćemo da jednačina

$$x^4 + y^4 = z^4 \tag{1.5}$$

nema rešenja u skupu prirodnih brojeva. Da bismo to dokazali, dokažimo prethodno sledeću lemu.

Lema 1.1 Jednačina

$$x^4 + y^4 = z^2 \tag{1.6}$$

nema rešenja u skupu prirodnih brojeva.

Dokaz. Dokaz ćemo izvesti metodom matematičke indukcije po prirodnom broju z.

Za $z=1$ tvrdjenje je očevidno tačno. Pretpostavimo da je tvrdjenje tačno za svako $z \leqslant z_o - 1$ i dokažimo da je tada tvrdjenje tačno za $z=z_o$.

Pretpostavimo obrnuto, neka za $z=z_o$ jednačina (1.6) ima rešenje $x=x_o$, $y=y_o$, tj. neka je

$$x_o^4 + y_o^4 = z_o^2. \qquad (1.7)$$

Razmotrimo dva slučaja: $(x_o, y_o, z_o) = d > 1$ i $(x_o, y_o, z_o) = 1$.

U prvom slučaju deljenjem sa d^4 jednačina (1.7) postaje

$$\left(\frac{x_o}{d}\right)^4 + \left(\frac{y_o}{d}\right)^4 = \left(\frac{z_o}{d^2}\right)^2,$$

gde je $z_o d^{-2} \in N$ i $z_o d^{-2} < z_o$, što protivreči induktivnoj pretpostavci da za svako $z < z_o$ jednačina (1.6) nema rešenja. U drugom slučaju iz (1.7), na osnovu teoreme 1.1, sledi

$$x_o^2 = 2ab, \quad y_o^2 = a^2 - b^2, \quad (a,b) = 1.$$

Očigledno, odabrali smo da je x_o paran, a y_o neparan broj. Na osnovu teoreme 1.1 sledi da je b parno i uz to

$$b = 2uv, \quad y_o = u^2 - v^2, \quad a = u^2 + v^2, \quad (u,v) = 1. \qquad (1.8)$$

Iz (1.8) sledi

$$x_o^2 = 2ab = 4uv(u^2 + v^2).$$

Kako je $(u,v) = 1$, to mora biti

$$u = x_1^2, \quad v = y_1^2, \quad u^2 + v^2 = z_1^2. \qquad (1.9)$$

Zamenjujući (1.9) u (1.8) dobijamo

$$a = z_1^2 = x_1^4 + y_1^4.$$

Znači, za $z = z_1 \leqslant a < x_o^2 \leqslant z_o$ jednačina (1.6) ima rešenje $x = x_1$, , $y = y_1$, što protivreči induktivnoj pretpostavci da jednačina (1.6) nema rešenja za svako $z < z_o$.

Dakle, u oba razmatrana slučaja došli smo do kontradikcije, pa zaključujemo da iz induktivne pretpostavke sledi da za $z = z_o$ jednačina (1.6) nema rešenja u skupu prirodnih brojeva. Time je prema principu matematičke indukcije lema u potpunosti dokazana.

Jednačina (1.5) može se napisati u obliku

$$x^4 + y^4 = (z^2)^2,$$

pa lema 1.1 direktno dokazuje sledeću teoremu.

Teorema 1.2 Jednačina (1.5) nema rešenja u skupu prirodnih brojeva.

Znači, za $n = 4$ Fermat-ovo tvrdjenje je bilo tačno.

1.3 Uvodno razmatranje opšteg slučaja Fermat-ovog problema

Razmatramo dakle, problem: da li jednačina

$$x^n + y^n = z^n, \quad n \geq 3 \tag{1.10}$$

ima rešenja u skupu prirodnih brojeva. Već smo pokazali da je za $n=4$ odgovor negativan. Naš sledeći korak biće da pokažemo da se rešavanje jednačine (1.10) može ograničiti na slučaj kada je n prost neparan broj.

Lema 1.2 Ako jednačina (1.10) nema rešenja za $x,y,z \in N$, $n \in P$, tada jednačina (1.10) nema rešenja za $x,y,z \in N$, $n \in N-P$.

Dokaz. Neka je $n \in N-P$, $n \geq 3$. Razmotrimo dva slučaja: prvi, ako je n oblika $n=2^k$, $k \geq 2$, i drugi, ako n nije tog oblika. Za $n=2^k$, $k \geq 2$, jednačina (1.10) se može napisati u obliku

$$\left(x^{2^{k-2}}\right)^4 + \left(y^{2^{k-2}}\right)^4 = \left(z^{2^{k-2}}\right)^4,$$

pa je na osnovu teoreme 1.2 lema dokazana.

Ako n nije oblika 2^k, tada postoji prost neparan broj p takav, da je $n=mp$. No, onda se jednačina (1.10) može napisati u obliku

$$(x^m)^p + (y^m)^p = (z^m)^p,$$

pa, opet, neposredno izlazi tvrdjenje leme.

Lema 1.2 nam očigledno dozvoljava, da umesto jednačine (1.10) posmatramo jednačinu

$$x^p + y^p = z^p, \quad p \in P, \quad p \geq 3. \tag{1.11}$$

Osim toga, mi ćemo u buduće smatrati da su u jednačini (1.11) x,y,z dva po dva relativno prosti. Naime, ako bi bilo $(x,y)=d>1$, sledilo bi $(x,y,z)=d$, pa bi se jednačina (1.11) mogla da skrati sa d^p.

Višegodišnjim proučavanjem Fermat-ovog problema, matematičari su došli do saznanja da je praktično razlikovati dva slučaja. Prvi, kada je $xyz \not\equiv o \pmod p$, tako zvani prvi slučaj Fermat-ovog problema, i drugi, kada je $xyz \equiv o \pmod p$, tako

zvani drugi slučaj Fermat-ovog problema.

Navedimo sad nekoliko osnovnih tvrdjenja vezanih za jednačinu (1.11).

Lema 1.3 Ako su x,y,z relativno prosti prirodni brojevi koji zadovoljavaju jednačinu (1.11) i ako je $xyz \not\equiv o \pmod p$, tada postoje $a,b,c \in N$ takvi da je

$$2x = a^p - b^p + c^p,\quad 2y = -a^p + b^p + c^p,\quad 2z = a^p + b^p + c^p,$$
$$x \equiv o \pmod a,\quad y \equiv o \pmod b,\quad z \equiv o \pmod c. \qquad (1.12)$$

Dokaz. Dokažimo, pre svega, da ako je $(x,y)=1$, da je tada najveća zajednička mera brojeva $x+y$ i $\frac{x^p + y^p}{x + y}$ jednaka 1 ili p. Stvarno, iz $x+y \equiv o \pmod d$, sledi

$$x^{p-1} - x^{p-2}y + \ldots + y^{p-1} \equiv px^{p-1} \pmod d,$$

a odavde izlazi da je $\frac{x^p + y^p}{x + y}$ deljivo sa d jedino za $d=p$.

Iz uslova leme iz $z \not\equiv o \pmod p$ sledi $x+y \not\equiv o \pmod p$, pa su $x+y$ $\frac{x^p + y^p}{x + y}$ relativno prosti. No, onda neposredno sledi da, pošto je proizvod dva relativno prosta broja p-ti stepen prirodnog broja z, mora biti

$$x+y = c^p,\quad z \equiv o \pmod c.$$

Analogno se dobija

$$z-x = b^p,\quad y \equiv o \pmod b,$$
$$z-y = a^p,\quad x \equiv o \pmod a.$$

Iz poslednjih jednakosti direktno sledi tvrdjenje (1.12).Time je lema u potpunosti dokazana.

Slično tvrdjenje važi i u drugom slučaju Fermat-ovog problema.

Lema 1.4 Ako su x,y,z relativno prosti brojevi koji zadovoljavaju jednačinu (1.11) i ako je $z \equiv o \pmod p$, tada postoje $a,b,c \in N$ takvi da je

$$2x = a^p - b^p + p^{2p-1}c^p,\quad 2y = -a^p + b^p + p^{2p-1}c^p,\quad 2z = a^p + b^p + p^{2p-1}c^p,$$
$$x \equiv o \pmod a,\quad y \equiv o \pmod b,\quad z \equiv o \pmod c. \qquad (1.13)$$

Dokaz. Kako je po pretpostavci $(x,z)=(y,z)=1$, to iz $z \equiv o$

(mod p), sledi $xy \not\equiv o \pmod p$, pa se slićno kao i u dokazu leme 1.3 dobija

$$z - x = b^p, \quad y \equiv o \pmod b, \tag{1.14}$$

$$z - y = a^p, \quad x \equiv o \pmod a. \tag{1.15}$$

Prema maloj Fermat-ovoj teoremi je $z^p = x^p + y^p \equiv x + y \pmod p$, pa iz $z \equiv o \pmod p$ sledi $x + y \equiv o \pmod p$. No, onda je, kao što smo pokazali u lemi 1.3, $x^{p-1} - x^{p-2}y + \ldots + y^{p-1}$ deljivo sa p, ali nije deljivo sa p^2. Znači, ako je $z = p^m c_1 z_1$, $c_1 z_1 \not\equiv o \pmod p$, $m \geq 1$, mora biti

$$x + y = p^{mp-1} c_1^p. \tag{1.16}$$

Iz jednakosti (1.14), (1.15) i (1.16) izlazi $2z = a^p + b^p + p^{mp-1} c_1^p$. Kako je $z \equiv o \pmod p$, to mora biti $a^p + b^p \equiv a + b \equiv o \pmod p$. No, onda je i $a^{p-1} - a^{p-2}b + \ldots + b^{p-1} \equiv o \pmod p$, pa je $a^p + b^p \equiv o \pmod{p^2}$. Po pretpostavci je $m \geq 1$, $p \geq 3$, pa je $mp-1 \geq 2$, tj.

$$2z = a^p + b^p + p^{mp-1} c_1^p \equiv o \pmod{p^2}.$$

Znači, $m \geq 2$, pa stavljajući u (1.16) $c = p^{m-2} c_1$ dobijamo

$$x + y = p^{2p-1} c^p, \quad z \equiv o \pmod c. \tag{1.17}$$

Iz (1.14), (1.15) i (1.17) direktno izlaze jednakosti (1.13). Time je lema u potpunosti dokazana.

Primetimo, da bi se slične jednakosti dobile da smo pretpostavili da je $x \equiv o \pmod p$, odnosno $y \equiv o \pmod p$.

Sledeća lema, koju dokazujemo, ne odnosi se direktno na Fermat-ov problem, već daje jedan rezultat iz teorije brojeva, kojeg ćemo kasnije vrlo često da koristimo.

Lema 1.5 Neka su $x, y \in N$, $(x,y)=1$. Tada, osim eventualno prostog broja $p \geq 3$, svi ostali prosti faktori brojeva

$$\frac{x^p - y^p}{x - y}, \quad \frac{x^p + y^p}{x + y}$$

su oblika $2kp+1$, $k \in N$.

Dokaz. Neka je

$$x^p - y^p \equiv o \pmod q, \quad x - y \not\equiv o \pmod q, \quad q \in P.$$

Po prostom modulu q postoji primitivni koren t, tj. postoji takav t da je $t^m \equiv 1 \pmod q$ ako i samo ako je $q-1 \mid m$. Kako je po pretpostavci $(x,y)=1$, $x-y \not\equiv o \pmod q$, to postoji $m<q-1$ takav da je

$$x \equiv t^m y \pmod q.$$

No, onda je

$$t^{mp} \equiv 1 \pmod q. \tag{1.18}$$

Iz (1.18) sledi da mp mora biti deljivo sa $q-1$, pa kako je $m<q-1$, mora biti $q-1 \equiv o \pmod p$, odnosno,

$$q = 2kp + 1, \quad k \in N.$$

Takodje, u dokazu leme 1.3 videli smo, broj $\frac{x^p - y^p}{x - y}$ može biti deljiv sa p, ali ne sa p^2.

Stavljajući $x \equiv - t^m y \pmod q$, analogno se izvodi dokaz i za broj $\frac{x^p + y^p}{x + y}$. Time je lema u potpunosti dokazana.

Lema 1.6 Neka su x,y,z rešenja jednačine (1.11) i neka je $xyz \not\equiv o \pmod p$. Neka su, dalje, a,b,c brojevi definisani sa (1.12), pri čemu je $x=ax_1$, $y=by_1$, $z=cz_1$. Tada važi:

a) Svi prosti faktori brojeva x_1,y_1,z_1 su oblika $2kp^2 + 1$, $k \in N$.

b) $x^{p-1} \equiv y^{p-1} \equiv z^{p-1} \equiv 1 \pmod{p^3}$.

Dokaz. a) Neka je $z_1 \equiv o \pmod q$. Prema lemi 1.3 biće $z-x=b^p$, $z-y=a^p$, odnosno

$$x \equiv - b^p, \quad y \equiv - a^p \pmod q.$$

Kako je $x+y=c^p$, $(c,z_1)=1$, to izlazi

$$a^p + b^p \not\equiv o \pmod q. \tag{1.19}$$

S druge strane je $x^p + y^p = z^p$, pa je

$$a^{p^2} + b^{p^2} \equiv o \pmod q. \tag{1.20}$$

Po prostom modulu q postoji primitivni koren t, dakle, postoji $m \leq q-1$ takav da je $a \equiv - t^m b \pmod q$. Kako iz (1.19) sledi $a+b \not\equiv o \pmod q$, to mora biti $m<q-1$. Iz (1.19) i (1.20) izlazi

$$t^{mp} \not\equiv 1 \pmod q, \quad t^{mp^2} \equiv 1 \pmod q. \tag{1.21}$$

Prema lemi 1.5 $q=2k_1p+1$, pa iz (1.21) izlazi

$$m \not\equiv o, \quad mp \equiv o \pmod{2k_1}.$$

No, onda je $k_1 \equiv o \pmod{p}$, tj. $k_1 = kp$, pa je $q = 2kp^2 + 1$, što je i trebalo dokazati.

Potpuno analogno dokazuje se tvrdjenje za proste faktore brojeva x_1, y_1.

b) Kako je $x_1 \equiv y_1 \equiv z_1 \equiv 1 \pmod{p^2}$, to je $x_1^p \equiv y_1^p \equiv z_1^p \equiv 1 \pmod{p^3}$, pa iz $(ax_1)^p + (by_1)^p = (cz_1)^p$ izlazi $a^p + b^p \equiv c^p \pmod{p^3}$. No, onda, na osnovu (1.12) važi

$$x \equiv a^p, \quad y \equiv b^p, \quad z \equiv c^p \pmod{p^3}, \tag{1.22}$$

odnosno,

$$a^{p-1} \equiv b^{p-1} \equiv c^{p-1} \equiv 1 \pmod{p^2}.$$

Sledi

$$a^{p(p-1)} \equiv b^{p(p-1)} \equiv c^{p(p-1)} \equiv 1 \pmod{p^3},$$

ili na osnovu (1.22)

$$x^{p-1} \equiv y^{p-1} \equiv z^{p-1} \equiv 1 \pmod{p^3}, \tag{1.23}$$

što je i trebalo dokazati.

Na osnovu prethodne leme može elementarno da se pokaže da za $p=3$ jednačina (1.11) nema rešenja relativno prosta sa 3. Stvarno, na osnovu (1.23) važi

$$x^2 \equiv y^2 \equiv z^2 \equiv 1 \pmod{9},$$

pa kako je $xyz \not\equiv o \pmod{3}$, to mora biti

$$x \equiv y \equiv -z \pmod{9}.$$

No, onda iz $x + y \equiv z \pmod{9}$ izlazi $3z \equiv o \pmod{9}$, što je nemoguće.

Jednačina (1.11), ili u krajnjoj liniji jednačina (1.10), može da se razmatra u svetlu izvesnih nejednakosti, koje x, y, z moraju da zadovoljavaju. Tako se u [36] navodi rezultat I.Paasche-a*:

Ako su x, y, z prirodni brojevi za koje je

$$x^2 - 1 \leqslant 2y,$$

---

* I.Paasche, Praxis der Mathematik, 3 (1961), 80. Za dokaz videti [36] 25-26.

tada je

$$x^n + y^n \neq z^n, \quad n \geq 3.$$

Mi ćemo pokušati da pokažemo nešto strožije tvrdjenje. Naime, važi sledeća lema.

Lema 1.7 Ako $x, y, z \in N$ zadovoljavaju jednačinu (1.10), tada mora biti

$$x^2 - 1 > ny, \quad n \geq 3. \tag{1.24}$$

Dokaz. Pre svega, dokažimo da za svako $t \geq n+1$ važi nejednakost

$$t^{n-1} > n^{n-2}(t+1), \quad n \geq 3. \tag{1.25}$$

Neka je $f(t) = t^{n-1} - n^{n-2}(t+1)$, tada je za $t \geq n+1$ $f'(t) > 0$, pa za $t > n+1$ funkcija $f(t)$ raste. Kako je

$$f(n+1) = (n+1)^{n-1} - n^{n-2}(n+2) > n^{n-1} + (n-1)n^{n-2} -$$

$$- n^{n-2}(n+2) = (n-3)n^{n-2} \geq 0,$$

to zaključujemo da za svako $t \geq n+1$, $n \geq 3$, važi $f(t) > 0$.

Dokažimo, dalje, da ako x, y, z zadovoljavaju jednačinu (1.10), tada važi $x > n$, $y > n$, $z > n$. Stvarno, ako je, na primer, $x < y < z$, tada sledi

$$x^n = z^n - y^n = (z-y)(z^{n-1} + z^{n-2}y + \ldots + y^{n-1}) > (z-y)ny^{n-1} > ny^{n-1},$$

odnosno, deljenjem sa xy^{n-1}

$$\frac{n}{x} < \left(\frac{x}{y}\right)^{n-1} < 1.$$

Sada nije teško dokazati tvrdjenje leme. Pretpostavimo obrnuto, neka $x, y, z \in N$ zadovoljavaju jednačinu (1.10) i neka je

$$x^2 - 1 \leq ny, \quad n \geq 3.$$

Uzimajući u obzir da mora biti $y \geq n+1$, što znači da y zadovoljava nejednačinu (1.25), sledi

$$y^n < z^n = x^n + y^n \leq (1+ny)^{\frac{n}{2}} + y^n < n^{\frac{n}{2}}(y+1)^{\frac{n}{2}} + y^n = n^{\frac{n}{2}}(y+1)^{\frac{n-1}{2}}(y+1)^{\frac{1}{2}} + y^n <$$

$$< n^{\frac{n}{2}}(y+1)^{\frac{n-1}{2}} n^{\frac{2-n}{2}} y^{\frac{n-1}{2}} + y^n = n\left[(y(y+1))^{\frac{n(n-1)}{2}}\right]^{\frac{1}{n}} + y^n =$$

$$= n\left[\prod_{k=0}^{n-1} y^k (1+y)^{n-1-k}\right]^{\frac{1}{n}} + y^n < \left[y^{n-1} + y^{n-2}(1+y) + \ldots + (1+y)^{n-1}\right] + y^n =$$

$$= \left[(1+y)^n - y^n\right] + y^n = (1+y)^n,$$

odnosno,

$$y < z < 1 + y,$$

što je nemoguće, jer je z prirodan broj. Time je lema u potpunosti dokazana.

Primetimo, da je direktna posledica gornje leme tvrdjenje, da za fiksirano x postoji najviše konačno mnogo trojki (y,z,n), takvih da je $x^n + y^n = z^n$. Naime, mora da važi (1.24), a takodje i $n<x$.

Sa ovim bi završili iznošenje nekih osnovnih činjenica vezanih za opšti slučaj Fermat-ovog problema. Naš sledeći korak biće da izložimo ideju Kummer-a i neke rezultate proistekle iz nje. Za takav postupak imamo dobro opravdanje. Sama ideja je briljantna, a rezultati proistekli iz nje, predstavljaju nesumnjivo najznačajnije rezultate postignute u tretiranju Fermat-ovog problema.

1.4 Neke algebarske strukture

Prinudjeni smo da pre izlaganja pomenutog Kummer-ovog rezultata damo u najkraćim crtama pregled nekih algebarskih struktura sa kojima se Kummer koristi u svom dokazu. Jasno je, da ćemo se zbog obilja teoretskog materijala vrlo često morati odreći dokaza navedenih teorema, no u krajnjoj liniji, te dokaze nije teško pronaći u navedenoj literaturi.

Definicija 1.1 Algebarski brojevi jesu rešenja algebarske jednačine $a_0 + a_1 x + \ldots + a_n x^n = o$, $a_i \in Q$, $i=0,1,2,\ldots n$, $n \in N$.

Definicija 1.2 Ceo algebarski broj jeste rešenje normirane algebarske jednačine sa koeficijentima iz D.

Definicija 1.3 Stepen algebarskog broja b je najmanji stepen normirane algebarske jednačine sa koeficijentima iz Q, koju broj b zadovoljava.

Definicija 1.4 Minimalan polinom $M(x)$ algebarskog broja b jeste normiran polinom stepena s, čiji je b koren. Pri tom, s je stepen broja b.

Nije teško videti da algebarski broj b ima jedan jedini minimalni polinom. Naime, kada bi $M(x)$ i $P(x)$ bila dva minimalna polinoma broja b, tada bi bilo $M(b)-P(b)=o$, što znači da je b koren polinoma $M(x)-P(x)$ stepena manjeg od s, pa izlazi $M(x) \equiv P(x)$.

Definicija 1.5 Norma algebarskog broja b, u oznaci $N(b)$, jeste proizvod svih nula minimalnog polinoma $M(x)$ broja b; pri tom se svaka nula računa svojom kratnošću.

Nameće se pitanje kakva je struktura skupa A algebarskih brojeva, odnosno, skupa EA celih algebarskih brojeva, s obzirom na operacije sabiranja i množenja. Odgovor na to pitanje proizlazi iz sledeće teoreme.

Teorema 1.3 Ako su b i c (celi) algebarski brojevi, a $f(x,y)$ bilo koji algebarski polinom nad Q (odnosno Z), tada je i broj $a=f(b,c)$ (ceo) algebarski broj. ([24], 1090-1092.)

Ako stavimo $f(x,y)=x+y$ i $f(x,y)=xy$, tada će neposredna posledica teoreme 1.3 biti da su $(A,+)$, $(A,\cdot)$, $(EA,+)$, $(EA,\cdot)$ grupoidi. Kada smo to konstatovali, preostali deo dokaza naredne teoreme je trivijalan.

Teorema 1.4 $(A,+,\cdot)$ je polje. $(EA,+,\cdot)$ je prsten.

Za nas će mnogo više biti od interesa proučavanje, ne polja A, nego nekih njegovih podpolja. Polje A očigledno sadrži neka podpolja; na primer, $Q \subset A$ i $(Q,+,\cdot)$ je polje. Isto tako,ako je $Q(\sqrt{2}) = \{ p+q\sqrt{2}: p,q \in Q\}$, tada je $(Q(\sqrt{2}),+,\cdot)$ polje; pri tom je očigledno $Q(\sqrt{2}) \subset A$. Medjutim, može da se dokaže mnogo opštija teorema.

Teorema 1.5 Ako je b bilo koji algebarski broj stepena s, tada skup $Q(b)$ svih vrednosti racionalnih funkcija u odnosu na b sa koeficijentima iz Q je polje. Svi celi algebarski brojevi koji su u $Q(b)$ čine prsten, pa čak i integralni domen. Pri tom, svaki element $a \in Q(b)$ ima jedinstven zapis oblika

$$a = a_o + a_1 b + \ldots + a_{s-1} b^{s-1},$$

gde je $a_i \in Q$, $i=0,1,\ldots,s-1$. ([24], 1093-1094.)

Na osnovu teoreme 1.5 lako se dokazuje da je $(Z[\zeta],+,\cdot)$

integralni domen, gde je $Z[\zeta]$ definisan sa

$$Z[\zeta]=\{a_0+ a_1\zeta +\ldots+ a_{p-2}\zeta^{p-2}: a_i\in D, \zeta = cos\frac{2\pi}{p} + i\, sin\frac{2\pi}{p}\}. \quad (1.26)$$

videćemo, ovaj integralni domen igraće u našem poslu vidnu ulogu.

Naš sledeći korak je da malo bolje upoznamo strukturu integralnog domena. Za početak, interesuje nas sledeće: da li integralni domen I ima takvih elemenata x da iz $x\in I\Rightarrow x^{-1}\in I$, i ako ima, kakva je struktura takvih elemenata. Na prvo pitanje odgovor je očevidno potvrdan. Naime, I je po definiciji prsten sa jedinicom e, a iz $e\in I$ sledi $e^{-1}= e\in I$. Medjutim, da li osim jedinice e integralni domen ima još koji element sa navedenim svojstvom, neizvesno je i zavisi od toga o kojem se integralnom domenu radi. Tako, na primer, u $(D,+,\cdot)$, osim $e=1$, još samo jedan element, -1, zadovoljava pomenuto svojstvo.

Definicija 1.6 Element x integralnog domena I naziva se jednotom, ako iz $x\in I$ sledi $x^{-1}\in I$.

Teorema 1.6 Ako je S skup svih jednotnih elemenata integralnog domena I, tada je $(S,\cdot)$ grupa. ([24], 1095-1096.).

Uvedimo još nekoliko pojmova vezanih za integralni domen.

Definicija 1.7 Element $a\in I$ je asociran (pridružen) elementu $b\in I$, ako je $a = \varepsilon b$ za neku jednotu $\varepsilon\in I$.

Definicija 1.8 Element x integralnog domena I je nerastavljiv ako je različit od 0, različit od svake jednote $\varepsilon\in I$, te ako je deljiv jedino sa ε i svakim svojim pridruženikom εx.

Definicija 1.9 Element $p\in I$ je prost ako $p|bc\Rightarrow p|b\vee p|c$. Pri tom, sa $p|x$ označavamo "p deli x".

Na prvi pogled, nameće se pomisao da u definicijama 1.8 i 1.9 definišemo jedan te isti pojam. Medjutim, to nije tačno, mada imamo dovoljno dobro opravdanje za takvu pomisao.U skupu D naime, u kojem mi nesvesno i zamišljamo pojam "prost broj", važi da je nerastavljivo isto što i prosto. Ali u opštem slučaju, može da se pokaže samo da iz pretpostavke da je p prost, sledi da je p nerastavljiv. Stvarno, neka je $p=mn$ i neka $p|mn\Rightarrow$

$\Rightarrow p \mid m \vee p \mid n$. Neka, na primer, $p \mid m$, tj. $m=pq$. No, onda je

$p=mn=(pq)n=p(qn)\Rightarrow qn=1\Rightarrow q=n^{-1}\Rightarrow n$ je jednota.

Da obrnuto tvrdjenje u opštem slučaju ne važi, pokazuje sledeći primer. U integralnom domenu $(D(\sqrt{-3}),+,\cdot)$ broj 2 je nerastavljiv, jer iz

$$2 = (x + y\sqrt{-3})(a + b\sqrt{-3}), \quad by \neq o$$

prelazeći na norme dobijamo

$$4 = N(x + y\sqrt{-3})N(a + b\sqrt{-3}) = (x^2 + 3y^2)(a^2 + 3b^2),$$

a poslednja jednačina ima rešenja u D jedino za $a + b\sqrt{-3} = 1$, pri čemu je 1 jedinica, pa dakle i jednota, u $D(\sqrt{-3})$. S druge strane, broj 2 nije prost jer $2 \mid (1+\sqrt{-3})(1-\sqrt{-3})$, a pri tom, $2 \nmid (1+\sqrt{-3})$ i $2 \nmid (1-\sqrt{-3})$.

U stvari, važi sledeća teorema.

Teorema 1.7 Ako je u integralnom domenu I faktorizacija u nerastavljive elemente jednoznačna, tada je element $p \in I$ prost ako i samo ako je nerastavljiv. ([24], 1097.)

Može nam se zameriti da razmatrajući ove, nesumnjivo interesantne, algebarske strukture zalutamo u oblast, koja sa teorijom brojeva nema neke naročite veze. Sledeći primer će brzo da nas u tome razuveri.

Rešimo jednačinu

$$x^2 - 2y^2 = 7 \qquad (1.27)$$

u skupu prirodnih brojeva. Nije teško probanjem ustanoviti da su $x=3$, $y=1$ i $x=5$, $y=3$ dva rešenja jednačine (1.27). Medjutim, naći sva rešenja jednačine (1.27) nije tako jednostavno. Da je kojim slučajem naš zadatak bio da rešimo jednačinu $x^2 - y^2 = 7$, mi bi, naslućujući, pisavši je u obliku $(x-y)(x+y)=7$, vrlo lako našli sva njena rešenja. I ideja se naslućuje. Forma $x^2 - 2y^2$ ne može istina da se faktoriše u integralnom domenu D, ali u integralnom domenu $D(\sqrt{2})$ može. Stvarno, u $D(\sqrt{2})$, jednačina (1.27) postaje

$$7 = x^2 - 2y^2 = (x + y\sqrt{2})(x - y\sqrt{2}) = N(x+y\sqrt{2}) = N(\alpha). \qquad (1.28)$$

Na taj način, naš zadatak se sveo na pronalaženje takvih $\alpha \in D(\sqrt{2})$ za koje je $N(\alpha)=7$. Ali to nije sve. Ako je $\varepsilon \in D(\sqrt{2})$ takav da je

$N(\varepsilon)=1$, tada je $N(\varepsilon^n)=1$, za svako $n\in N$, pa je $N(\alpha)=N(\alpha)N(\varepsilon^n)=N(\alpha\varepsilon^n)$. No, to znači, da ako je α jedno rešenje jednačine (1.28), da su tada i $\alpha\varepsilon^n$, gde je $N(\varepsilon)=1$, rešenja jednačine (1.28).

Preostalo je, dakle, da se nadje postupak za odredjivanje onih elemenata iz $D(\sqrt{2})$ čija je norma 1. Istina, u našem slučaju može da se uoči da je $\varepsilon=3+2\sqrt{2}$, ali kako stoji stvar u opštem slučaju? Očigledno, od odgovora na to pitanje, zavisi efikasnost uočenog postupka u rešavanju Diofantovih jednačina uopšte.

Definicija 1.10 Neka je K polje algebarskih brojeva stepena n i neka je

$$M = \{c_1\alpha_1 + c_2\alpha_2 + \ldots + c_m\alpha_m : \quad c_i\in D,\ \alpha_i\in K,\quad 1\leqslant i\leqslant m\}.$$

M se naziva poretkom polja K ako su ispunjeni sledeći uslovi:

1° U skupu M postoji tačno n linearno nezavisnih elemenata.

2° $(M,+,\cdot)$ je integralni domen.

Teorema 1.8 Neka je M poredak polja K. Element $\varepsilon\in M$ je jednota ako i samo ako je $N(\varepsilon) = \pm 1$.

Dokaz. Iz definicije 1.10 proizlazi da minimalni polinom broja $\alpha\in M$ ima cele koeficijente, tj. svi elementi u M su celi algebarski brojevi. Pokažimo, pre svega, da je u integralnom domenu M $N(\alpha)$ deljivo sa α za svako $\alpha\in M$. Neka je

$$f(x) = x^n + c_1x^{n-1} + \ldots + c_n, \quad c_i\in D,\quad i=1,2,\ldots,n$$

minimalni polinom broja α. Kako je $f(\alpha)=0$, to sledi

$$\frac{N(\alpha)}{\alpha} = \frac{(-1)^n c_n}{\alpha} = (-1)^{n-1}(\alpha^{n-1} + c_1\alpha^{n-2} + \ldots + c_{n-1})\in M,$$

tj. $N(\alpha)$ je deljivo sa α u M.

Ako je sad $N(\alpha)= \pm 1$, tada je 1 deljivo sa α, pa sledi α je jednota. Obrnuto, ako je ε jednota, tada je $\varepsilon\varepsilon^{-1}= 1$, pa je $N(\varepsilon)N(\varepsilon^{-1})=1$, odnosno $N(\varepsilon)=\pm 1$.

Time je sve rečeno. Postupak rešavanja jednačina sličnih našem primeru (1.27), u svetlu iznetih algebarskih struktura, jasno je i precizno zacrtan. Jednačinu treba faktorisati u nekom poretku M polja algebarskih brojeva K i problem se, kao što smo pokazali, svodi na odredjivanje onih elemenata iz M čija je

norma *1*, ili, na osnovu teoreme 1.8 na odredjivanje jednota integralnog domena *M*. Ideja je, mora se priznati, stvarno briljantna.

Sve bi bilo u najboljem redu, kada pred nas ne bi iznenada iskrsao jedan ozbiljan problem. Pozovimo opet u pomoć jedan primer da objasnimo o čemu je reč.

Posmatrajmo integralni domen $D(\sqrt{-5})$. Nije teško utvrditi da su $\varepsilon=\pm 1$ jedine njegove jednote. Rastavimo broj *9* na nerastavljive faktore u $D(\sqrt{-5})$. Imamo

$$9 = 3\cdot 3 = (2+\sqrt{-5})(2-\sqrt{-5}).$$

Lako se može utvrditi da je svaki od brojeva 3, $2\pm\sqrt{-5}$ nerastavljiv. Isto tako, sva tri broja su medjusobno neasocirana, pošto ni jedan ne izlazi iz drugog množenjem sa jednotama $\varepsilon=\pm 1$. Zaključak je: u integralnom domenu $D(\sqrt{-5})$ faktorizacija nije jednoznačna.

Ideju kako da zaobidjemo iskrsli problem dao je Kummer. Ideja se sastoji u tome, što ako u integralnom domenu M nekog polja algebarskih brojeva faktorizacija nije jednoznačna, tada se svi elementi različiti od nule iz M mogu preslikati u neki nov skup, u kojem je definisano množenje i u kojem je faktorizacija jednoznačna. Sam Kummer nazvao je te nove objekte idealnim brojevima. Mi ćemo ih zvati divizorima.

Definicija 1.11 Neka je $(M,+,\cdot)$ integralni domen i neka je $M'=M-\{0\}$. Neka je, dalje $(G,\cdot)$ polugrupa sa jediničnim elementom u kojoj je faktorizacija na proste faktore jednoznačna i neka je $\alpha\to(\alpha)$ homomorfizam polugrupe $(M',\cdot)$ u polugrupu $(G,\cdot)$ koji zadovoljava sledeće uslove:

1° U integralnom domenu M element $\alpha\in M'$ deljiv je sa $\beta\in M'$ ako i samo ako je (α) deljivo sa (β) u polugrupi G.

2° Ako su za $\alpha,\beta\in M'$ (α) i (β) deljivi sa $a\in G$, tada su $(\alpha\pm\beta)$ takodje deljivi sa a.

3° Ako je skup svih elemenata $\alpha\in M'$, takvih da je (α) deljivo sa $a\in G$, jednak skupu svih elemenata $\beta\in M'$, takvih da je (β) deljivo sa $b\in G$, tada je $a=b$.

Tada polugrupu G sa zadanim homomorfizmom nazivamo teorijom divizora integralnog domena M, a njene elemente divizorima integralnog domena M. Divizore oblika (α), $\alpha\in M'$ nazivamo glavnim divizorima. Jedinični element e polugrupe G je jedinični divizor.

Nije teško utvrditi da je neposredna posledica uslova 1^{o} gornje definicije da jednakost $(\alpha)=(\beta)$ važi tada i samo tada kada su α i β asocirani u integralnom domenu M. No, onda iz $\alpha=\varepsilon\beta$, gde je ε jednota u M sledi

$$(\alpha)=(\varepsilon\beta)=(\varepsilon)(\beta)=(\varepsilon)(\alpha)\Rightarrow(\varepsilon)=e.$$

Znači, za sve jednote $\varepsilon\in M$ važi $(\varepsilon)=e$.

Može se s pravom postaviti pitanje, koliko je definicija 1.11 efikasna, naime, da li za svaki integralni domen M postoji teorija divizora, i ako postoji, da li je ona jedinstvena. Imajući na umu da nas u biti zanimaju polja algebarskih brojeva i njihovi maksimalni poretci, to sledeće dve teoreme daju u potpunosti odgovor na postavljena pitanja.

Teorema 1.9 Ako za integralni domen M postoji teorija divizora, tada je ona jedinstvena. ([2], 229-231.)

Teorema 1.10 Za maksimalni poredak M proizvoljnog polja algebarskih brojeva K postoji teorija divizora. ([2], 259-260.)

Navedimo još nekoliko pojmova i činjenica vezanih za teoriju divizora.

Definicija 1.12 Dva divizora a i b polja algebarskih brojeva K su ekvivalentna, u oznaci $a\sim b$, ako je $a=b(\alpha)$, $\alpha\in K$. Skup svih divizora polja K ekvivalentnih datom divizoru a naziva se klasom divizora i označava se sa $[a]$.

Jasno je da je $[a]=[b]$ ako i samo ako $a\sim b$. Takodje,ako stavimo $[a]\cdot[b] \overset{def.}{=} [ab]$,tada je skup svih klasa divizora komutativna grupa, s obzirom na ovako definisanu operaciju. Jedinični element te grupe je očevidno klasa $[e]$, a inverzni element klase $[a]$ je $[a^{-1}]$. Ako bi se poslužili terminima teorije grupa, jasno je da je grupa klasa divizora faktor grupa grupe svih divizora podgrupe glavnih divizora.

Grupa klasa divizora i njen red daju nam vrlo važne informacije o karakteristikama polja K. Ako je broj klasa divizora jednak 1, to znači, da su svi divizori glavni, a to opet znači da je u maksimalnom poretku M polja K faktorizacija jednoznačna. Dakle, vrlo često će se postavljati pitanje o broju klasa divizora nekog polja algebarskih brojeva. Navedimo jednu teo-

remu koja daje delimičan odgovor na to pitanje.

Teorema 1.11 Grupa klasa divizora proizvoljnog polja algebarskih brojeva je konačna. ([2], 293-294.)

Sa ovim bi naš kratak pregled nekih algebarskih struktura bio završen. Naoružani dovoljnim brojem podataka, možemo odlučnije da se uhvatimo u koštac sa tvrdjenjima koja će nas na kraju dovesti do našeg glavnog cilja: Kummer-ovog rezultata u rešavanju Fermat-ovog problema.

1.5 Nekoliko važnih lema

Prve četiri leme koje navodimo, odnose se na integralni domen $Z[\zeta]$ definisan sa (1.26) u odeljku 1.4, pri čemu ćemo smatrati da je $p \in P$, $p \geqslant 3$.

Lema 1.8 U integralnom domenu $Z[\zeta]$ broj $1-\zeta$ je nerastavljiv i za $p \in P$ važi faktorizacija

$$p = \varepsilon(1-\zeta)^{p-1}, \tag{1.29}$$

gde je ε jednota u $Z[\zeta]$.

Dokaz. Ako u jednakost

$$t^{p-1} + t^{p-2} + \ldots + 1 = (t-\zeta)(t-\zeta^2)\ldots(t-\zeta^{p-1})$$

stavimo $t=1$, dobijamo

$$p = \prod_{k=1}^{p-1} (1-\zeta^k). \tag{1.30}$$

Neka je $r(t)$ proizvoljni polinom sa racionalnim koeficijentima, tada za element $\alpha \in Q(\zeta)$, $\alpha = r(\zeta)$ važi*

$$N(\alpha) = \prod_{k=1}^{p-1} r(\zeta^k).$$

Stavljajući $\alpha = 1-\zeta^s$, $s \not\equiv 0 \pmod p$, dobijamo

$$N(1-\zeta^s) = \prod_{k=1}^{p-1} (1-\zeta^{ks}) = \prod_{k=1}^{p-1} (1-\zeta^k) = p. \tag{1.31}$$

---

* [2], 528-531.

Iz (1.31) sledi da su brojevi $1-\zeta^s$, $1<s\leqslant p-1$ nerastavljivi u $Z[\zeta]$. Stvarno, ako je $1-\zeta^s = ab$, tada je

$$N(1-\zeta^s) = N(ab) = N(a)N(b) = p,$$

pa kako je p prost to je ili $N(a)$, ili $N(b)$ jednako 1. No, onda prema teoremi 1.8 ili a, ili b je jednota.

Neka je dalje

$$1-\zeta^s = (1-\zeta)(1+\zeta+\ldots+\zeta^{s-1}) = (1-\zeta)\varepsilon_s.$$

Prelazeći na norme, dobijamo

$$p = N(1-\zeta^s) = N(1-\zeta)N(\varepsilon_s) = pN(\varepsilon_s) \Rightarrow N(\varepsilon_s) = 1.$$

Sledi, ε_s su jednote, pa iz (1.30) dobijamo

$$p = \prod_{k=1}^{p-1} (1-\zeta^k) = (1-\zeta)^{p-1} \prod_{k=1}^{p-1} \varepsilon_k = \varepsilon(1-\zeta)^{p-1},$$

a to je i trebalo dokazati.

Lema 1.9 Ako je broj $n \in D$, deljiv sa $1-\zeta$ u $Z[\zeta]$, tada je on deljiv i sa prostim brojem p.

Dokaz. Neka je $n=(1-\zeta)a$, $a \in Z[\zeta]$.Predjemo li na norme, dobijamo $n^{p-1} = N(1-\zeta)N(a)$. Prema lemi 1.8 $N(1-\zeta)=p$, tj. $n^{p-1} = pN(a)$. Kako je $Z[\zeta]$ maksimalni poredak, to su svi njegovi elementi celi algebarski brojevi, pa je $N(a) \in D$. Sledi, n je deljivo sa $p \in P$, što je i trebalo dokazati.

Lema 1.10 Svaka jednota u $Z[\zeta]$ je oblika $\nu\zeta^k$, gde je ν realna jednota.

Dokaz. Neka je

$$\varepsilon = a_o + a_1\zeta + \ldots + a_{p-2}\zeta^{p-2} = r(\zeta)$$

proizvoljna jednota u $Z[\zeta]$. Očigledno, konjugovan broj $\overline{\varepsilon}$ broju ε takodje će biti jednota u $Z[\zeta]$, pri čemu je

$$\overline{\varepsilon} = r(\zeta^{-1}) = r(\zeta^{p-1}).$$

Razmotrimo jednotu $\mu = \frac{\varepsilon}{\overline{\varepsilon}} \in Z[\zeta]$. Kako je $|\mu| = 1$, to mora biti

$$\mu = \pm \zeta^n, \quad n \in N. \tag{1.32}$$

Pokažimo da na desnoj strani jednakosti (1.32) mora da stoji znak +. Pretpostavimo suprotno, neka je $\mu = -\zeta^n$, tj. neka je

$\varepsilon = -\overline{\varepsilon}\zeta^n$. Kako je $\zeta \equiv 1 \pmod{1-\zeta}$, to je $\zeta^s \equiv 1 \pmod{1-\zeta}$, $1 \leqslant s \leqslant p-2$, pa je

$$\varepsilon \equiv \overline{\varepsilon} \equiv a_o + a_1 + \ldots + a_{p-2} = M \pmod{1-\zeta}. \qquad (1.33)$$

No, onda iz $\varepsilon = -\overline{\varepsilon}\zeta^n$ sledi $M \equiv -M \pmod{1-\zeta}$, odnosno $M \equiv 0 \pmod{1-\zeta}$, pa iz (1.33) izlazi $\varepsilon \equiv o \pmod{1-\zeta}$, što protivreči pretpostavci da je ε jednota.

Dakle, mora biti $\mu = \zeta^n$. Neka je k takav broj da je $2k \equiv n \pmod{p}$. Tada imamo

$$\varepsilon = \overline{\varepsilon}\zeta^n = \overline{\varepsilon}\zeta^{2k} \Rightarrow \frac{\varepsilon}{\zeta^k} = \overline{\varepsilon}\zeta^k = \frac{\overline{\varepsilon}}{\zeta^{-k}} = \overline{\left(\frac{\varepsilon}{\zeta^k}\right)}.$$

Znači, $\nu = \frac{\varepsilon}{\zeta^k} = \overline{\nu}$, pa $\nu \in R$ i uz to $\varepsilon = \nu\zeta^k$, a to je i trebalo dokazati.

Napomenimo da je lemu 1.10 prvi dokazao Kummer.

Lema 1.11 Neka su $x, y \in D$ i neka je $n \not\equiv 0 \pmod{p}$. Brojevi $x+\zeta^m y$ i $x+\zeta^n y$ su relativno prosti ako i samo ako je ispunjeno:

1^o x i y su relativno prosti.

2^o $x + y \not\equiv o \pmod{p}$.

Dokaz. Neka su $x+\zeta^m y$ i $x+\zeta^n y$ relativno prosti. Ako pretpostavimo da x i y imaju zajednički delitelj $d>1$, tada je očevidno $x+\zeta^m y \equiv x+\zeta^n y \equiv o \pmod{d}$, što je nemoguće. Takodje, ako pretpostavimo da je $x+y \equiv o \pmod{p}$, tada je $x+y \equiv o \pmod{1-\zeta}$, pa zbog

$$x + \zeta^m y = x + y + (\zeta^m - 1)y,$$

$$x + \zeta^n y = x + y + (\zeta^n - 1)y,$$

zaključujemo $x+\zeta^m y \equiv x+\zeta^n y \equiv o \pmod{1-\zeta}$, što je nemoguće. Time je u jednom smeru dokaz izveden.

Pretpostavimo sad da važi 1^o i 2^o. Treba dokazati da u $Z[\zeta]$ postoje takvi brojevi a_o i b_o da važi

$$(x + \zeta^m y)a_o + (x + \zeta^n y)b_o = I. \qquad (1.34)$$

Neka je S skup definisan na sledeći način

$$S = \{(x+\zeta^m y)a + (x+\zeta^n y)b : a, b \in Z[\zeta]\}.$$

Očigledno, ako $\alpha, \beta \in S$ tada i $c_1\alpha + c_2\beta \in S$, $c_1, c_2 \in Z[\zeta]$. Da dokažemo (1.34) treba dokazati da $1 \in S$. Kako je

$$(x+\zeta^m y)-(x+\zeta^n y)=\zeta^m(1-\zeta^{n-m})y=\varepsilon\zeta^m(1-\zeta)y=\varepsilon_1(1-\zeta)y,$$

$$(x+\zeta^m y)\zeta^n-(x+\zeta^n y)\zeta^m=-\zeta^m(1-\zeta^{n-m})x=-\varepsilon\zeta^m(1-\zeta)x=-\varepsilon_1(1-\zeta)x,$$

to zaključujemo $(1-\zeta)x$, $(1-\zeta)y \in S$.

Po pretpostavci 1° postoje u i v takvi da je

$$xu + yv = 1,$$

odnosno,

$$(1-\zeta)xu + (1-\zeta)yv = 1-\zeta,$$

pa $1-\zeta \in S$. Pošto je prema lemi 1.8

$$p = \varepsilon(1-\zeta)^{p-1} = \varepsilon(1-\zeta)^{p-2}(1-\zeta) + 0(1-\zeta),$$

to $p \in S$. Takodje iz

$$x+y = (x+\zeta^m y) + (1-\zeta^m)y = (x+\zeta^m y) + \varepsilon(1-\zeta)y$$

sledi $x+y \in S$. Prema uslovu 2° postoje u_1, v_1 takvi da je

$$(x+y)u_1 + pv_1 = 1.$$

No, to znači da $1 \in S$, što smo i hteli da dokažemo. Time je lema u potpunosti dokazana.

Sledeće tri leme odnose se na teoriju divizora, preciznije, na broj klasa divizora.

Lema 1.12 Ako je broj klasa divizora polja algebarskih brojeva h, tada je za svaki divizor a, a^h glavni divizor.

Dokaz. Poznato je da je red konačne grupe deljiv sa redom svakog elementa te grupe. Neka je a proizvoljni divizor. Tada je $[a]^h$ jedinični element grupe klasa divizora, tj. $[a^h]=[e]$. No, to znači da je a^h glavni divizor, što je i trebalo dokazati.

Lema 1.13 Ako broj klasa divizora h, polja algebarskih brojeva nije deljiv sa prostim brojem p i ako je divizor a^p glavni, tada je divizor a takodje glavni.

Dokaz. Kako su h i p relativno prosti, to postoje $u,v \in D$, takvi da je $hu+pv=1$. Divizor a^p je po pretpostavci glavni, a divizor a^h je glavni prema lemi 1.12. No, onda su i divizori a^{hu} i a^{pv} takodje glavni, pa je glavni i divizor $a^{hu}\cdot a^{pv} = a^{hu+pv} = a$, što je i trebalo dokazati.

Definicija 1.13 Proste neparne brojeve p, za koje broj klasa

divizora polja $Q(\zeta)$, $\zeta = cos\,\frac{2\pi}{p} + i \cdot sin\,\frac{2\pi}{p}$, nije deljiv sa p, nazivamo regularnim. Svi ostali prosti brojevi su iregularni.

Lema 1.14 Neka je p regularan prost broj. Ako je neka jednota ε polja $Q(\zeta)$ kongruentna po modulu p sa celim racionalnim brojem, tada je $\varepsilon=\varepsilon_1^p$, gde je ε_1 takodje jednota u $Q(\zeta)$. ([2], 496-497.)

Konačno, sve pripreme su obavljene i naš sledeći korak biće da formulišemo i dokažemo Kummer-ov rezultat.

1.6 Kummer-ova teorema

Teorema 1.12 Za regularne proste brojeve $p\geqslant 3$ jednačina

$$x^p + y^p = z^p \tag{1.35}$$

nema rešenja u skupu celih brojeva različitih od nule.

Dokaz. Razmatraćemo odvojeno prvi i drugi slučaj Fermat-ovog problema. Dakle, pretpostavimo prvo da suprotno iskazu teoreme, postoje celi relativno prosti brojevi x,y,z takvi da je $x^p + y^p = z^p$, $xyz \not\equiv o \pmod p$.

Kao što smo videli u odeljku 1.3, posledica leme 1.6 je bila da za $p=3$ jednačina (1.35) nema rešenja relativno prosta sa 3. Neka je, dakle, $p>3$. U integralnom domenu $Z[\zeta]$, polja $Q(\zeta)$, jednačinu (1.35) možemo napisati u obliku

$$\prod_{k=o}^{p-1} (x+\zeta^k y) = z^p. \tag{1.36}$$

Kako je $x + y \equiv x^p + y^p = z^p \equiv z \pmod p$ $z \not\equiv o \pmod p$, to je i $x+y \not\equiv o \pmod p$. No, onda prema lemi 1.11 $x+\zeta^m y$ i $x+\zeta^n y$, $m \not\equiv n \pmod p$, su relativno prosti, pa postoje $\beta,\gamma \in Z[\zeta]$, takvi da je

$$(x+\zeta^m y)\beta + (x+\zeta^n y)\gamma = 1. \tag{1.37}$$

Iz (1.37) sledi da su glavni divizori $(x+\zeta^k y)$, $o\leqslant k\leqslant p-1$, dva po dva relativno prosti. Prema (1.36) njihov proizvod je p-ti stepen divizora (z), pa izmedju ostalog mora biti

$$(x + \zeta y) = a^p, \tag{1.38}$$

gde je a divizor integralnog domena $Z[\zeta]$. Prema uslovu teoreme p je prost regularan broj, tj. broj klasa divizora polja $Q(\zeta)$

nije deljiv sa p, pa prema lemi 1.13 divizor a je glavni, tj. $a=(\alpha)$, $\alpha \in Z[\zeta]$. Tada iz (1.38) sledi

$$x + \zeta y = \varepsilon \alpha^p, \tag{1.39}$$

gde je ε jednota u $Z[\zeta]$.

Neka je

$$\alpha = a_o + a_1\zeta + \ldots + a_{p-2}\zeta^{p-2}, \quad M = a_o + a_1 + \ldots + a_{p-2},$$

tada je

$$\alpha^p \equiv a_o^p + a_1^p\zeta^p + \ldots + a_{p-2}^p\zeta^{p(p-2)} \equiv M \pmod{p}. \tag{1.40}$$

Prema lemi 1.10 svaka jednota ε može biti predstavljena u obliku $\nu\zeta^k$, gde je ν realna jednota. No, onda iz (1.39) i (1.40) sledi

$$x + \zeta y \equiv \nu\zeta^k M = \mu\zeta^k \pmod{p}, \tag{1.41}$$

gde je $\mu=\nu M \in R$.

Primetimo da za proizvoljno $\alpha \in Z[\zeta]$, konjugovan broj $\overline{\alpha} \in Z[\zeta]$. Takodje, iz $\alpha \equiv \beta \pmod{p}$, tj. $\alpha-\beta= p\gamma$, sledi $\overline{\alpha}-\overline{\beta}=p\overline{\gamma}$, tj. $\overline{\alpha} \equiv \overline{\beta} \pmod{p}$. Iskoristimo li to u kongruenciji (1.41) dobijamo

$$x + \zeta^{-1}y \equiv \overline{\mu}\zeta^{-k}. \tag{1.42}$$

Kako je $\mu \in R$, to $\mu=\overline{\mu}$, pa iz (1.41) i (1.42) sledi

$$x\zeta^k + y\zeta^{k-1} - x\zeta^{-k} - y\zeta^{1-k} \equiv o \pmod{p}. \tag{1.43}$$

Prodiskutujmo kongruenciju (1.43). Pre svega, ako je proizvoljni element iz $Z[\zeta]$ predstavljen u obliku $a_o + a_1\zeta + \ldots + a_{p-2}\zeta^{p-2}$ deljiv sa p, tada moraju svi a_i, $o \leqslant i \leqslant p-2$, biti deljivi sa p. Znači, ako na levoj strani kongruencije (1.43) medju eksponentima $k, k-1, -k, 1-k$ nema kongruentnih sa $p-1$ po modulu p, kao i ako su oni dva po dva nekongruentni po modulu p, tada iz (1.43) sledi $x \equiv y \equiv o \pmod{p}$, što protivreči pretpostavci $xyz \not\equiv o \pmod{p}$. Razmotrimo preostale dve mogućnosti.

Ako medju eksponentima $k, k-1, -k, 1-k$ ima kongruentnih sa $p-1$ po modulu p, tada zbog uslova $p>3$ iz tablice

k	$p-1$	o	1	2
$k-1$	$p-2$	$p-1$	o	1
$-k$	1	o	$p-1$	$p-2$
$1-k$	2	1	o	$p-1$

sledi da je samo jedan od navedenih eksponenata kongruentan sa $p-1$ po modulu p. Kako je

$$\zeta^{p-1} = -1 - \zeta - \ldots - \zeta^{p-2},$$

to nakon zamene odgovarajućeg sabirka u (1.43) dobijamo kongruenciju oblika

$$a(-1-\zeta-\ldots-\zeta^{p-2}) + b\zeta^m + c\zeta^n + d\zeta^s \equiv 0 \pmod{p}, \quad (1.44)$$

gde je $m,n,s \in \{k,k-1,-k,1-k\}$, $a,b,c,d \in \{x,-x,y,-y\}$. U zagradi na levoj strani kongruencije (1.44) ima $p-1 \geq 4 > 3$ sabirka, pa nakon sredjivanja po stepenima ζ, ostaje bar jedan sabirak sa koeficijentom $\pm x$ ili $\pm y$. Sledi, $x \equiv o$ ili $y \equiv o \pmod{p}$, što je nemoguće.

Preostaje još da razmotrimo slučaj kada medju eksponentima $k,k-1,-k,1-k$ ima medjusobno kongruentnih po modulu p. Kongruencije $k \equiv k-1$ i $-k \equiv 1-k \pmod{p}$ su očevidno nemoguće. Kongruencije $k \equiv -k$ i $k-1 \equiv 1-k \pmod{p}$ daju redom $k \equiv o$, $k \equiv 1 \pmod{p}$, odnosno, $k-1 \equiv p-1$, $-k \equiv p-1 \pmod{p}$, a to smo već razmatrali. Na kraju, korguencije $k \equiv 1-k$ $k-1 \equiv -k \pmod{p}$ daju $k \equiv \frac{p+1}{2} \pmod{p}$, pa (1.43) postaje

$$(x-y)\zeta^{\frac{p+1}{2}} + (y-x)\zeta^{\frac{p-1}{2}} \equiv o \pmod{p}. \quad (1.45)$$

Iz (1.45) sledi

$$x \equiv y \pmod{p}. \quad (1.46)$$

Ako jednačinu (1.35) zapišemo u obliku $x^p + (-z)^p = (-y)^p$, analogno se dobija

$$x - \zeta z = \varepsilon_1 \alpha_1^p. \quad (1.47)$$

Na isti način kao što smo iz (1.39) izveli (1.46), iz (1.47) izlazi

$$x \equiv -z \pmod{p}. \quad (1.48)$$

Iz (1.46) i (1.48) sledi

$$-x \equiv z \equiv z^p = x^p + y^p \equiv x + y \equiv 2x \pmod{p},$$

odnosno, zbog $p>3$, $x \equiv o \pmod{p}$, što opet protivreči pretpostavci $xyz \not\equiv o \pmod{p}$. Time je u prvom slučaju Fermat-ovog problema teorema dokazana.

Neka je sad $xyz \equiv o \pmod{p}$ i neka relativno prosti

celi brojevi x,y,z (različiti od nule) zadovoljavaju jednaćinu (1.35). Ne umanjujući opštost, možemo pretpostaviti da je $z \not\equiv o \pmod p$. U protivnom, ako bi, recimo, bilo $y \equiv o \pmod p$, jednačinu (1.35) bi mogli da zapišemo u obliku $x^p + (-z)^p = (-y)^p$.

Neka je $z = p^k z_o$, $k \geq 1$, $(z_o, p)=1$. Prema lemi 1.8 važi $p = \varepsilon(1-\zeta)^{p-1}$, gde je ε jednota u $Q(\zeta)$. Znači, u polju $Q(\zeta)$ jednačinu (1.35) možemo napisati u obliku

$$x^p + y^p = \varepsilon(1-\zeta)^{mp} z_o^p, \tag{1.49}$$

gde je $m=k(p-1)>o$.

Da dokažemo navode teoreme, dovoljno je dokazati da je jednakost oblika (1.49) nemoguće za $x,y,z_o \in D-\{o\}$. Mi ćemo dokazati nešto više. Dokazaćemo da je jednakost (1.49) nemoguća za $x,y,z_o \in Z[\zeta]$, pri čemu je $xyz_o \not\equiv o \pmod{1-\zeta}$.

Pretpostavimo obrnuto, neka je jednakost oblika (1.49) moguća, tada od svih jednakosti tog oblika izaberimo onu za koju je $m \geq 1$ najmanje. Neka je to baš jednakost (1.49).

Ako faktorišemo jednakost (1.49) i predjemo na jednakost sa divizorima dobijamo

$$\prod_{k=o}^{p-1} (x+\zeta^k y) = b^{mp} a^p, \tag{1.50}$$

gde je $b=(1-\zeta)$, $a=(z_o)$, $(a,b)=1$. Kako je $mp \geq p > o$, to je bar jedan od faktora na levoj strani jednakosti (1.50) deljiv sa b. S druge strane, iz

$$x + \zeta^k y = x + \zeta^n y - \zeta^n(1 - \zeta^{k-n})y$$

sledi

$$(x + \zeta^k y) \equiv (x + \zeta^n y) \pmod b,$$

pa su svi divizori $(x+\zeta^k y)$, $o \leq k \leq p-1$, deljivi sa b.

Primetimo dalje, da je za $o \leq k < n \leq p-1$ kongruencija

$$(x + \zeta^k y) \equiv (x + \zeta^n y) \pmod{b^2} \tag{1.51}$$

nemoguća. Stvarno, ako bi važilo (1.51), sledilo bi

$$\zeta^k y(1 - \zeta^{n-k}) \equiv o \pmod{(1-\zeta)^2},$$

što je nemoguće, jer je $1-\zeta^{n-k}$ asocirano sa $1-\zeta$, a po pretpostavci je $(y, 1-\zeta)=1$.

Znači, $\frac{(x+\zeta^k y)}{b}$, $o<k<p-1$, čini punu sistemu ostataka po modulu b, pa kako je $N(b)=p$, to je jedan i samo jedan od $(x+\zeta^k y)$ deljiv sa b^2. Pošto se, u krajnjoj liniji, može svuda umesto y pisati $\zeta^k y$, to ne umanjujući opštost možemo smatrati da je baš $(x+y) \equiv o \pmod{b^2}$. Znači, $p-1$ divizor $(x+\zeta^k y)$, $1\leqslant k\leqslant p-1$, je deljiv sa b i nije deljiv sa b^2, a divizor $(x+y)$ je deljiv b^2. Sledi, leva strana jednakosti (1.50) je deljiva sa b^{p+1}, pa izlazi $m>1$.

Neka je d najveća zajednička mera divizora (x) i (y). Kako (x) i (y) nisu deljivi sa b, to ni d nije deljivo sa b. Jasno je, da su $(x+\zeta^k y)$, $1\leqslant k\leqslant p-1$ deljivi sa bd, a da je $(x+y)$ deljivo sa $b^{p(m-1)+1}d$. Drugim rečima,

$$(x + y) = c_o d b^{p(m-1)+1}, \tag{1.52}$$

$$(x + \zeta^k y) = c_k d b, \quad 1\leqslant k\leqslant p-1. \tag{1.53}$$

Dokažimo da su divizori c_i, $o\leqslant i\leqslant p-1$, dva po dva uzajamno prosti. Stvarno, ako bi c_k i c_n, $k\neq n$, imali zajednički delitelj c, tada bi iz deljivosti $(x+\zeta^k y)$ i $(x+\zeta^n y)$ sa bcd sledilo da su i divizori $(\zeta^k y)(1-\zeta^{k-i})=b(y)$ i $(x)(1-\zeta^{k-i})=b(x)$ deljivi sa bcd, što znači da je $(x) \equiv (y) \equiv o \pmod{cd}$, a to protivreči pretpostavci da je $d = ((x),(y))$.

Uzimajući u obzir (1.52) i (1.53) jednakost (1.50) postaje

$$d^p \prod_{k=o}^{p-1} c_k = a^p.$$

Kako su c_k dva po dva relativno prosti, to sledi $c_k = a_k^p$, $o\leqslant k\leqslant p-1$. No, onda, jednakosti (1.52) i (1.53) postaju

$$(x + y) = a_o^p d b^{p(m-1)+1}, \tag{1.54}$$

$$(x + \zeta^k y) = a_k^p d b, \quad 1\leqslant k\leqslant p-1. \tag{1.55}$$

Izrazimo d iz (1.54) i zamenimo u (1.55). Dobijamo

$$(x + \zeta^k y) b^{p(m-1)} = (x + y)(a_k a_o^{-1})^p. \tag{1.56}$$

Kako su $(x+\zeta^k y)$, $o\leqslant k\leqslant p-1$ i $b=(1-\zeta)$ glavni divizori, to iz (1.56) sledi da je i divizor $(a_k a_o^{-1})^p$ glavni. Po pretpostavci p je regularan prost broj, pa je prema lemi 1.13 i divizor $a_k a_o^{-1}$ glavni.

Znači, $\alpha_k \alpha_o^{-1} = \left(\frac{\alpha_k}{\beta_k}\right)$, gde su $\alpha_k, \beta_k \in Z[\zeta]$. Pri tome, iz $\alpha_k \alpha_o \not\equiv o \pmod{b}$, izlazi $(\alpha_k)(\beta_k) \not\equiv o \pmod{b}$.

Iz (1.56), vraćajući se na jednakosti u $Z[\zeta]$, dobijamo

$$(x+\zeta^k y)(1-\zeta)^{p(m-1)} = (x+y)\left(\frac{\alpha_k}{\beta_k}\right)\varepsilon_k, \quad 1 \leq k \leq p-1, \tag{1.57}$$

gde su ε_k jednote u $Z[\zeta]$. Množeći jednakost

$$(x+\zeta y)(1+\zeta) - (x+\zeta^2 y) = \zeta(x+y)$$

sa $(1-\zeta)^{p(m-1)}$, uzimajući u obzir (1.57) za $k=1$ i $k=2$, dobijamo

$$(x+y)\left(\frac{\alpha_1}{\beta_1}\right)^p \varepsilon_1(1+\zeta) - (x+y)\left(\frac{\alpha_2}{\beta_2}\right)^p \varepsilon_2 = (x+y)\zeta(1-\zeta)^{p(m-1)},$$

odnosno

$$(\alpha_1\beta_2)^p - \frac{\varepsilon_2}{\varepsilon_1(1+\zeta)}(\alpha_2\beta_1)^p = \frac{\zeta}{\varepsilon_1(1+\zeta)}(1-\zeta)^{p(m-1)}(\beta_1\beta_2)^p. \tag{1.58}$$

Jednakost (1.58) je oblika

$$\alpha^p + \varepsilon_o \beta^p = \varepsilon'(1-\zeta)^{p(m-1)}\gamma^p, \tag{1.59}$$

gde su $\alpha, \beta, \gamma \in Z[\zeta]$, ε_o, ε' jednote u $Z[\zeta]$.

Videli smo da je $m-1>o$, tj. $p(m-1) \geq p$, pa iz (1.59) sledi

$$\alpha^p + \varepsilon_o \beta^p \equiv o \pmod{(1-\zeta)^p}. \tag{1.60}$$

Kako je $\beta \not\equiv o \pmod{1-\zeta}$, to postoji β' takav da je $\beta\beta' \equiv 1 \pmod{1-\zeta}$, pa iz (1.60) dobijamo

$$\varepsilon_o \equiv (-\alpha\beta')^p = \omega^p \pmod{(1-\zeta)^p} \tag{1.61}$$

Iz (1.61), zbog $N(1-\zeta)=p$, izlazi $\varepsilon_o \equiv M \pmod{p}$, gde je M ceo racionalni broj. Po pretpostavci p je regularan prost broj, pa je prema lemi 1.14 $\varepsilon_o = \mu^p$ gde je μ jednota u $Z[\zeta]$. No, onda, konačno, (1.59) postaje

$$\alpha^p + (\mu\beta)^p = \varepsilon'(1-\zeta)^{p(m-1)}\gamma^p. \tag{1.62}$$

Jednakost (1.62) je istog oblika kao i jednakost (1.49), s tom razlikom, što se u eksponentu na desnoj strani jednakosti umesto m nalazi $m-1$, što je nemoguće, jer smo pretpostavili da smo u (1.49) izabrali najmanje moguće m. Time je teorema dokazana i u drugom slučaju Fermat-ovog problema, pa je samim tim dokaz u potpunosti završen.

Izloženi rezultat Kummer-a nesumnjivo pleni svojom idejom. No i pored toga, može se s pravom postaviti pitanje, koliko je taj rezultat objektivno značajan. U takvoj jednoj proceni presudnu ulogu igraju dva momenta. Prvi, u uspostavljanju dovoljno efikasnog kriterijuma za utvrdjivanje da li je neki prost broj regularan, i drugi, u utvrdjivanju koliko uopšte ima regularnih prostih brojeva.

Sam Kummer je postavio dovoljno jednostavan kriterijum za utvrdjivanje regularnosti prostog broja.

Teorema 1.13 Prost broj $p \geq 3$ regularan je ako i samo ako važi $B_m \not\equiv 0 \pmod{p}$, za svako $m=2,4,6,\ldots p-3$, gde su B_m Bernoulli-jevi brojevi. ([2], 485-496.)

Pri tom su Bernoulli-jevi brojevi racionalni brojevi definisani sa

$$\frac{t}{e^t-1} = 1 + \sum_{n=1}^{\infty} \frac{B_n}{n!}\, t^n.$$

Napomenimo, da će o Bernoulli-jevim brojevima biti mnogo više reči u odeljku 1.8, kada će, izmedju ostalog, biti objašnjeno zašto se u izvesnim kongruencijama sa njima može da barata kao da su celi brojevi.

U svojim prvim radovima Kummer je postavio hipotezu da iregularnih prostih brojeva ima samo konačno mnogo. Medjutim, koristeći upravo Kummerove rezultate, Jensen je tu hipotezu oborio ([2], 502-503), dokazavši da iregularnih prostih brojeva ima beskonačno mnogo. Da li regularnih prostih brojeva ima beskonačno mnogo, za sada nije poznato.

Činjenica je da medju prostim brojevima ≤ 4001 ima 216 iregularnih i 334 regularna. Od prostih brojeva manjih od 100, jedino su 37, 59, 67 iregularni.

Dakle, bez obzira na originalnost i lepotu Kummer-ove ideje, stoji činjenica da je i dalje Fermat-ov problem nerešen za beskonačno mnogo prostih brojeva.

Naš sledeći korak biće da se upoznamo sa najznačajnijim rezultatima postignutim u tretiranju prvog slučaja Fermat-ovog problema. Tu su, kao što ćemo da vidimo, postignuti znatno bolji rezultati nego u opštem slučaju.

1.7 Prvi slučaj Fermat-ovog problema

Jedan od najznačajnijih rezultata vezanih za prvi slučaj Fermat-ovog problema dao je opet Kummer. On je, koristeći dalju izgradnju teorije divizora, izveo vrlo jak kriterijum za utvrdjivanje pod kojim uslovima jednačina

$$x^p + y^p = z^p, \quad p \in P, \quad p \geq 3 \tag{1.63}$$

može da ima rešenja relativno prosta sa p. To je tako zvana Kummer-ova lema, koja u formulaciji Mirimanoff-a glasi ovako.

Teorema 1.14 Da bi jednačina (1.63) imala rešenja relativno prosta sa p potrebno je da svih šest brojeva

$$\frac{x}{z}, \frac{z}{x}, \frac{y}{z}, \frac{z}{y}, -\frac{x}{y}, -\frac{y}{x} \tag{1.64}$$

zadovoljava svih $\frac{p-1}{2}$ kongruencija

$$B_{p-k} f_k(v) \equiv 0 \pmod{p}, \quad k=3,5,7,\ldots p-2,p-1, \tag{1.65}$$

gde su B_{p-k} Bernoulli-jevi brojevi, a $f_k(v)$ polinomi

$$f_k(v) = 1^{k-1}v + 2^{k-1}v^2 + \ldots + (p-1)^{k-1}v^{p-1} = \sum_{m=1}^{p-1} m^{k-1}v^m. \tag{1.66}$$

([7], II, 744-745, 761.)

Teorema 1.14 dovela je do niza veoma dobrih rezultata. Cauchy je iz nje izvukao uslov: Da bi jednačina (1.63) imala rešenja relativno prosta sa p, potrebno je da važi

$$B_{p-3} \equiv 0 \pmod{p} \tag{1.67}$$

([7],II,741). Kummer je poboljšao rezultat Cauchy-ja dokazavši da mora istovremeno da važi

$$B_{p-3} \equiv 0 \pmod{p}, \quad B_{p-5} \equiv 0 \pmod{p} \tag{1.68}$$

([7],II,741). Kasnije, Mirimanoff je pokazao da mora biti istovremeno

$$B_{p-k-1} \equiv 0 \pmod{p}, \quad k=2,4,6,8 \tag{1.69}$$

([7],II,742).

Tačku na niz rezultata ovakvog tipa stavio je Frobenius [22], dokazavši da postoji p_o (koji može biti efektivno izračunat) takav da za $p \geq p_o$ jednačina (1.63) može imati rešenja relativno prosta sa p samo pod uslovom

$$B_{p-k-1} \equiv 0 \pmod{p}, \tag{1.70}$$

za svako $k=2,4,\ldots,2k_o$, $k_o=[\sqrt{\ln p}]$. Ovaj rezultat se smatra jednim od najboljih rezultata postignutim do sada u tretiranju prvog slučaja Fermat-ovog problema ([45],[59]).

S druge strane, niz matematičara je iz teoreme 1.14 izvuklo uslov: Da bi jednačina (1.63) imala rešenja relativno prosta sa p, potrebno je da važi

$$q^{p-1} \equiv 1 \pmod{p^2}, \tag{1.71}$$

za sve proste brojeve q, $2 \leq q \leq 31$. Uslov (1.71) izvodjen je postepeno u vremenskom periodu od tridesetak godina, pri čemu su svoj doprinos dali Wieferich [63] za $q=2$, Mirimanoff [35] $q=3$, Vandiver [53] $q=5$, Frobenius [13] $q=11,17$, Polaczek [43], Morishima [39] i Rosser [46]-[48] za $q \leq 31$. Napomenimo, da su poslednja dvojica izveli uslov (1.71) i za $q \leq 43$, ali su (prema [45]) u njihovim dokazima pronadjeni izvesni nedostaci.

Mi ćemo se u IV glavi ponovo vratiti na teoremu 1.14, kojom prilikom ćemo dokazati teoremu ekvivalentnu njoj. Ta teorema će nam omogućiti da poboljšamo rezultate (1.67)-(1.70), kao i da izvedemo uslov (1.71) za $q=2$.

Od drugih rezultata vezanih za prvi slučaj Fermat-ovog problema, pomenućemo još tri. Vandiver je dokazao da ako broj klasa divizora h polja $Q(\zeta + \zeta^{-1}) = Q(2\cos\frac{2\pi}{p})$, $\zeta = \cos\frac{2\pi}{p} + i\sin\frac{2\pi}{p}$, nije deljiv sa p, tada jednačina (1.63) nema rešenja relativno prosta sa p ([57]). Neizvesno je da li postoje prosti brojevi p za koje bi h bilo deljivo sa p. Provereno je da medju prostim brojevima ≤ 4001 takvih nema ([2],298).

Krasner je dao još jedan interesantan rezultat. On je u [23] pokazao da ako postoji bar jedan $q=2kp+1 \in P$, takav da je

$$k \not\equiv 0 \pmod{p},\ 2^{2k} \not\equiv 1 \pmod{q},\ 3^k < q^2, \tag{1.72}$$

tada jednačina (1.63) nema rešenja relativno prosta sa p.

Konačno, spomenimo nesumnjivo značajan rezultat Brückner-a. On je 1975 godine, koristeći rezultat Eichler-a ([10]), dokazao da ako jednačina (1.63) ima rešenja relativno prosta sa

p, tada mora biti

$$ii(p) \geq \sqrt{p} - 2, \tag{1.73}$$

gde je $ii(p)$ indeks iregularnosti broja p, tj. broj Bernoulli-jevih brojeva B_{2k}, $2k<p-1$, deljivih sa p ([5]).

Ovde bi bilo interesantno uporediti ovaj Brückner-ov rezultat sa rezultatom Krasner-a, datim sa (1.70). Jasno je da je $\sqrt{p}-2$ esencijalno veće od $[\sqrt[3]{\ln p}]$. Medjutim, u Krasner-ovom uslovu se zahteva da $[\sqrt[3]{\ln p}]$ uzastopnih parnih Bernoulli-jevih brojeva (i to počevši od B_{p-3} na niže) bude deljivo sa p, dok se u Brückner-ovom uslovu uzastopnost ne zahteva, što je suštinski različito. Na taj način, i pored Brückner-ovog rezultata, rezultat Krasner-a ima i dalje svoju vrednost.

1.8 Bernoulli-jevi brojevi

Već smo u prethodna dva odeljka videli da su u neposrednoj vezi sa Fermat-ovim problemom Bernoulli-jevi brojevi. Kako ćemo sa njima imati i kasnije posla, razmotrimo ovde neke njihove osobine.

Definicija 1.14 Bernoulli-jevi brojevi B_m, $m \geq 1$, su racionalni brojevi odredjeni razvojem*

$$\frac{t}{e^t - 1} = 1 + \sum_{m=1}^{\infty} \frac{B_m}{m!} t^m. \tag{1.74}$$

Kako je funkcija

$$\frac{t}{e^t - 1} + \frac{t}{2} = 1 + \sum_{m=2}^{\infty} \frac{B_m}{m!} t^m$$

parna, to je $B_{2m+1} = 0$ za svako $m \in N$. Takodje, zapisavši (1.74) u obliku

$$t = \left(1 + \sum_{m=1}^{\infty} \frac{B_m}{m!} t^m\right) \sum_{m=1}^{\infty} \frac{t^m}{m!},$$

uporedjujući koeficijente uz t^m, lako se dokazuje sledeća lema.

---

* U delu literature se pod Bernoulli-jevim brojevima podrazumevaju brojevi $b_m = (-1)^{m-1} B_{2m}$. U suštini je svejedno, pošto je $B_{2m+1} = 0$, $m \geq 1$.

Lema 1.15 Za svako $n \geq 2$, Bernoulli-jevi brojevi zadovoljavaju rekurentnu vezu

$$(I + B)^m - B_m, \tag{1.75}$$

gde je $B^n = B_n$, $n \in \mathbb{N}$. ([2], 504.)

Iz (1.72) neposredno izlazi

$$B_1 = -\frac{1}{2}, \quad B_2 = \frac{1}{6}, \quad B_4 = -\frac{1}{30}, \quad B_6 = \frac{1}{42}, \ldots$$

Izvedimo sad za B_m jednu manje poznatu rekurentnu vezu od veze (1.75).

Lema 1.16 Za svako $m \in \mathbb{N}$ važi

$$(\frac{1}{2} + B)^m = (\frac{1}{2^{m-1}} - 1)B_m. \tag{1.76}$$

Dokaz. Iz (1.74), množenjem sa $e^{\frac{t}{2}}$, dobijamo

$$\frac{te^{\frac{t}{2}}}{e^t - 1} = (1 + \sum_{m=1}^{\infty} \frac{B_m}{m!} t^m)(1 + \sum_{m=1}^{\infty} \frac{t^m}{2^m m!}). \tag{1.77}$$

Koeficijent uz t^m u (1.77) je

$$a_m = \frac{1}{2^m m!} + \frac{B_1}{2^{m-1} 1!(m-1)!} + \frac{B_2}{2^{m-2} 2!(m-2)!} + \ldots + \frac{B_m}{m!} =$$

$$= \frac{1}{m!} \left[B_m + \binom{m}{1}\frac{1}{2} B_{m-1} + \ldots + \binom{m}{m-1}\frac{1}{2^{m-1}} B_1 + \frac{1}{2^m}\right] =$$

$$= \frac{1}{m!} (\frac{1}{2} + B)^m. \tag{1.78}$$

S druge strane je

$$\frac{te^{\frac{t}{2}}}{e^t - 1} = \frac{te^{\frac{t}{2}} + t - t}{e^t - 1} = 2\frac{e^{\frac{t}{2}}}{e^{\frac{t}{2}} - 1} - \frac{t}{e^t - 1} =$$

$$= 2(1 + \sum_{m=1}^{\infty} \frac{B_m}{m!} (\frac{t}{2})^m) - (1 + \sum_{m=1}^{\infty} \frac{B_m}{m!} t^m) =$$

$$= 1 + \sum_{m=1}^{\infty} \frac{B_m}{m!} (\frac{1}{2^{m-1}} - 1) t^m. \tag{1.79}$$

Uzimajući u obzir (1.78), iz (1.79) sledi (1.76), što je i trebalo dokazati.

Vezani sa Bernoulli-jevim brojevima su i sume $S_k(n)$, određene sa

$$S_k(n) = 1^k + 2^k + 3^k + \ldots + (n-1)^k, \quad k \in N, \; n \in N, \; n \geq 2.$$

Nije teško dokazati sledeće osobine sume $S_k(n)$ ([2], 505-507).

Lema 1.17 Neka je p prost broj. Tada je

$$S_k(p) \equiv \begin{cases} -1, & p-1 \mid k \\ 0, & p-1 \nmid k \end{cases} \pmod p.$$

Lema 1.18 Za svako $m \in N$ važi jednakost

$$(m+1)S_m(n) = (n+B)^{m+1} - B_{m+1}. \tag{1.80}$$

Sada možemo da dokažemo, za nas vrlo značajnu, Staudt--ovu teoremu.

Teorema 1.15 Neka je p prost, a m paran broj. Ako $p-1$ ne deli m, tada je B_m p-celo (tj. B_m ne sadrži p u imeniocu). Ako pak, $p-1$ deli m, tada je pB_m p-celo, pri čemu je

$$pB_m \equiv -1 \pmod p. \tag{1.81}$$

Dokaz. Teoremu ćemo da dokažemo metodom matematičke indukcije po m. Za $m=2$, $B_2 = \frac{1}{6}$, pa je tvrdjenje očigledno tačno. Pretpostavimo da je tvrdjenje tačno za svako $m=2,4,\ldots 2n-2$ i dokažimo da je tvrdjenje tačno za prirodan broj $m=2n$.

Prema lemi 1.18 važi

$$(2n+1)S_{2n}(p) = (p+B)^{2n+1} - B_{2n+1},$$

odnosno,

$$pB_{2n} = S_{2n}(p) - \sum_{k=0}^{2n-1} \frac{1}{2n+1} \binom{2n+1}{k} p^{2n-k} pB_k. \tag{1.82}$$

Dokažimo da su svi članovi koji stoje pod znakom sume u jednakosti (1.82) p-celi. Faktor pB_k je p-ceo, jer je za k neparno $B_k = 0$, $k>1$, $B_1 = -\frac{1}{2}$, a za k parno po induktivnoj pretpostavci. Ispitajmo faktor

$$N = \frac{1}{2n+1}\binom{2n+1}{k} p^{2n-k} = \frac{1}{2n+1}\binom{2n+1}{2n+1-k} p^{2n-k} = \frac{2n(2n-1)\ldots(k+1)}{(2n-k+1)!} p^{2n-k}.$$

Za $p=2$, N je očigledno p-ceo broj. Za $p \neq 2$, broj p ulazi u $r! = (m-k+1)!$ sa eksponentom

$$\left[\frac{r}{p}\right]+\left[\frac{r}{p^2}\right]+\ldots < \frac{r}{p}+\frac{r}{p^2}+\ldots = \frac{r}{p-1} < \frac{r}{2} < r-1 < m-1.$$

Sledi, N je prazan broj deljiv sa p, pa iz (1.82) izlazi

$$pB_{2n} \equiv S_{2n}(p) \pmod{p}. \tag{1.83}$$

Na osnovu leme 1.17, iz (1.83) izlazi

$$pB_{2n} \equiv \begin{cases} -1, & p-1 \mid 2n \\ 0, & p-1 \nmid 2n \end{cases} \pmod{p}.$$

Time je dokazano da iz pretpostavke da je tvrdjenje tačno za svako $m=2,4,\ldots 2n-2$, sledi da je ono tačno za $m=2n$, pa prema principu matematičke indukcije zaključujemo da je tvrdjenje tačno za svako parno $m \in N$. Time je teorema u potpunosti dokazana.

Teorema 1.15 dozvoljava nam, da u slučaju kada $p-1$ ne deli m, sa brojevima B_m baratamo u kongruencijama po modulu p kao da su B_m celi brojevi. Ovu važnu činjenicu imali smo i imaćemo stalno na umu.

II G L A V A

2.1 Polazna teorema

Već smo istakli u Uvodu da je u [51] (38-41) dokazana teorema: Ako je bar jedan od brojeva $2p+1$, $4p+1$ prost, tada jednačina

$$x^p + y^p = z^p, \quad x,y,z \in N \tag{2.1}$$

nema rešenja relativno prosta sa p. Naš zadatak biće da ovaj rezultat pokušamo da generališemo.

Temelj našeg daljeg rada biće sledeća teorema.

Teorema 2.1 Neka je $q=sp+1$ prost broj, $p \in P$, $p \geqslant 3$, i neka kongruencije

$$t^s \equiv 1 \pmod q, \quad (t+1)^s \equiv 1 \pmod q \tag{2.2}$$

nemaju zajedničko rešenje. Tada, ako je

$$s^s \not\equiv 1 \pmod q \tag{2.3}$$

onda jednačina (2.1) nema rešenja relativno prosta sa p.

Dokaz. Pretpostavimo obrnuto, neka pod datim uslovima jednačina (2.1) ima rešenja relativno prosta sa p.

Dokažimo, pre svega, da mora biti $xyz \equiv o \pmod q$. Stvarno, ako bi bilo $xyz \not\equiv o \pmod q$, tada bi postojao t, takav da je $y^p \equiv tx^p \pmod q$. Iz (2.1) sledi

$$y^{sp} \equiv 1 \equiv t^s x^{sp} \equiv t^s \pmod q,$$

$$(tx^p + x^p)^s = (t+1)^s x^{sp} \equiv (t+1)^s \equiv z^{sp} \equiv 1 \pmod q,$$

odnosno

$$t^s \equiv (t+1)^s \equiv 1 \pmod q,$$

što protivreči pretpostavci da par kongruencija (2.2) nemaju zajedničko rešenje. Dakle, $xyz \equiv o \pmod q$. Ne umanjujući opštost možemo pretpostaviti da je $x \equiv o \pmod q$.

Prema lemi 1.3 postoje a,b,c takvi da je

$2x = a^p - b^p + c^p$, $x \equiv o \pmod a$, $y \equiv o \pmod b$, $z \equiv o \pmod c$.

Znači, mora biti

$$a^p + c^p \equiv b^p \pmod q. \qquad (2.4)$$

Kongruencija (2.4) je istog tipa kao već razmatrana kongruencija $x^p + y^p \equiv z^p \pmod q$, pa mora biti $abc \equiv o \pmod q$. Kako su x,y,z relativno prosti i $x \equiv o \pmod q$, to mora biti $a \equiv o \pmod q$. No, onda, na osnovu leme 1.3 sledi

$$y \equiv z \equiv b^p \equiv c^p \pmod q. \qquad (2.5)$$

Kako je $z-y=a^p$, to iz (2.5) sledi

$$(\frac{x}{a})^p = \frac{z^p - y^p}{z - y} \equiv py^{p-1} \equiv p(b^{p-1})^p \pmod q,$$

odnosno

$$(\frac{x}{a})^{sp} \equiv 1 \equiv p^s(b^{p-1})^{sp} \equiv p^s \pmod q,$$

ili, nakon množenja sa s^s

$$s^s \equiv (sp)^p \equiv (-1)^s = 1 \pmod q. \qquad (2.6)$$

Medjutim, (2.6) je direktno u suprotnosti sa uslovom (2.3), pa smo mi ponovo došli do kontradikcije. Time je teorema u potpunosti dokazana.

Primetimo da je neposredna posledica teoreme 2.1 tvrdjenje izneto na početku odeljka. Naime, za $s=2$, iz $t^2 \equiv (t+1)^2 \equiv 1 \pmod{q=2p+1}$, sledi $2^2 \equiv 1 \pmod q$, odnosno, $q=3$, $p=1$, što je nemoguće. Takodje za $s=4$, iz $t^4 \equiv (t+1)^4 \equiv 1 \pmod{q=4p+1}$, sledi redom

$$t^4 \equiv 1 \wedge 4t^3 + 6t^2 + 4t + 1 \equiv 0 \wedge 6t^3 + 4t^2 + t + 4 \equiv 0$$

$$\pmod q \Rightarrow 5(2t^2 + 2t - 1) \equiv 0 \wedge t^4 \equiv 1 \pmod q \Rightarrow$$

$$\Rightarrow 5(1-8t) \equiv 0 \wedge t^4 \equiv 1 \pmod q \Rightarrow 8^4 \equiv 1 \pmod q \Rightarrow$$

$$\Rightarrow 5 \cdot 7 \cdot 9 \cdot 13 \equiv 0 \pmod q \Rightarrow p=3.$$

Već iz ove kratke ilustracije postaje jasno da se za $s>4$, recimo već za $s=8$, račun vrlo brzo komplikuje, što znači, da moramo da ustanovimo neke generalnije metode za rešavanje para kongruencija (2.2). Zato će naši napori biti usmereni upravo u tom pravcu.

2.2 Determinante $A_{n,r}$, $B_{m,n,r}$, $C_{n,r}$, $D_{m,n,r}$

Glavnu ulogu u rešavanju problema postavljenog u prethodnom odeljku igraće izvestan broj cikličkih i kosocikličkih determinanti. Konkretno, definišimo sledeće.

Definicija 2.1 Neka je $n \geqslant 5$ neparan broj, $2 \leqslant r \leqslant n-1$. Pod $A_{n,r}$, $C_{n,r}$ podrazumevaćemo sledeće cikličke determinante n-tog reda

$$A_{n,r} = -\begin{vmatrix} -1 & & & 1 & & -1 \\ -1 & \ddots & & & \iddots & \\ & \ddots & & & & \\ & & & \mathbf{0} & & \\ & & & & \ddots & 1 \\ 1 & & & & & \\ & \ddots & & & & \\ \mathbf{0} & & 1 & & -1 & -1 \end{vmatrix}, \qquad (2.7)$$

($n-r+1$-va kolona)

$$C_{n,r} = \frac{1}{3}\begin{vmatrix} 1 & & & 1 & & 1 \\ 1 & \ddots & & & \iddots & \\ & \ddots & & & & \\ & & & \mathbf{0} & & \\ & & & & \ddots & 1 \\ 1 & & & & & \\ & \ddots & & & & \\ \mathbf{0} & & 1 & & 1 & 1 \end{vmatrix}. \qquad (2.8)$$

($n-r+1$-va kolona)

Definicija 2.2 Neka je $m \geqslant 2$ prirodan, a $n \geqslant 1$ neparan broj, $2^m n > 4$. Pod $B_{m,n,r}$ podrazumevaćemo kosocikličku determinantu $2^{m-1}n$ -tog reda

$$B_{m,n,r}=\begin{vmatrix} & & \overset{2^{m-1}n-r+1-va\ kolona}{} & & \\ -1 & & -1 & & 1 \\ -1 & & & \mathbf{O} & \\ & & \mathbf{O} & & -1 \\ 1 & & & & \\ & \mathbf{O} & & & \\ \mathbf{O} & & & & \\ & & 1 & -1 & -1 \end{vmatrix}, \quad r=3,5,\ldots\ 2^{m-1}n-3, \tag{2.8}$$

$$B_{m,n,r}=\begin{vmatrix} -1 & & 1 & & 1 \\ -1 & & & \mathbf{O} & \\ & & \mathbf{O} & & 1 \\ -1 & & & & \\ & \mathbf{O} & & & \\ \mathbf{O} & & & & \\ & & -1 & -1 & -1 \end{vmatrix}, \quad r=2^{m-1}n+3, 2^{m-1}n+5,\ldots 2^{m}n-1. \tag{2.9}$$

Definicija 2.3 Neka je $m\geqslant 3$ prirodan, a $n\geqslant 5$ neparan broj, $r=1,3,\ldots 2^{m-1}-1$. Neka je dalje

$$b_i=\sum_{j=o}^{\infty}(-1)^j\binom{n}{2^{m-1}j+i},\quad a_i=\begin{cases} b_i, & i\neq r \\ b_i-1, & i=r \end{cases},\quad 0\leqslant i\leqslant 2^{m-1}-1.$$

Pod $D_{m,n,r}$ podrazumevaćemo kosocikličku determinantu 2^{m-1}-og reda

$$D_{m,n,r}=\begin{vmatrix} a_o & -a_2 & -1 & -a_2 & -2 & \cdots & -a_1 \\ a_1 & a_o & & -a_2 & -1 & \cdots & -a_2 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ a_2 & -1 & a_2 & -2 & a_2 & -3 & \cdots & a_o \end{vmatrix}. \tag{2.10}$$

Da bi izračunali u opštem slučaju determinante odredjene definicijama 2.1-2.3 dokažimo jednu značajnu osobinu koju imaju cikličke, odnosno, kosocikličke determinante.

Lema 2.1 Za cikličku determinantu

$$D = \begin{vmatrix} a_1 & a_2 & a_3 & \dots & a_n \\ a_n & a_1 & a_2 & \dots & a_{n-1} \\ a_{n-1} & a_n & a_1 & \dots & a_{n-2} \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ a_2 & a_3 & a_4 & \dots & a_1 \end{vmatrix} \tag{2.11}$$

važi

$$D = \prod_{k=1}^{n} f(\zeta_k), \tag{2.12}$$

gde je $\zeta_k = \sqrt[n]{1} = cos\ \frac{2k\pi}{n} + i\,sin\ \frac{2k\pi}{n}$, $k=1,2,\dots n$, $f(x) = a_1 + a_2x + \dots + a_{n-1}x^{n-2} + a_nx^{n-1}$.

Dokaz. Označimo sa V determinantu Vandermond-a sa elementima $\zeta_1, \zeta_2, \dots \zeta_n$, gde su ζ_k sve vrednosti $\sqrt[n]{1}$. Dakle,

$$V = \begin{vmatrix} 1 & 1 & 1 & \dots & 1 \\ \zeta_1 & \zeta_2 & \zeta_3 & \dots & \zeta_n \\ \zeta_1^2 & \zeta_2^2 & \zeta_3^2 & \dots & \zeta_n^2 \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ \zeta_1^{n-1} & \zeta_2^{n-1} & \zeta_3^{n-1} & \dots & \zeta_n^{n-1} \end{vmatrix}.$$

Množenjem determinanata dobijamo

$$DV = \begin{vmatrix} a_1 + a_2\zeta_1 + \dots + a_n\zeta_1^{n-1} & \dots & a_1 + a_2\zeta_n + \dots + a_n\zeta_n^{n-1} \\ a_n + a_1\zeta_1 + \dots + a_{n-1}\zeta_1^{n-1} & \dots & a_n + a_1\zeta_n + \dots + a_{n-1}\zeta_n^{n-1} \\ \cdot & \cdot & \cdot \\ a_2 + a_3\zeta_1 + \dots + a_1\zeta_1^{n-1} & \dots & a_2 + a_3\zeta_n + \dots + a_1\zeta_n^{n-1} \end{vmatrix}.$$

Množenjem prve kolone sa ζ_1^{n-1}, druge sa ζ_2^{n-1} ... n-te sa ζ_n^{n-1}, vodeći računa da je $\zeta_k^n = 1$ za svako $k=1,2,\dots n$, dobijamo

$$DV = \begin{vmatrix} f(\zeta_1)\zeta_1^{n-1} & f(\zeta_2)\zeta_2^{n-1} & \dots & f(\zeta_n)\zeta_n^{n-1} \\ f(\zeta_1) & f(\zeta_2) & \dots & f(\zeta_n) \\ f(\zeta_1)\zeta_1 & f(\zeta_2)\zeta_2 & \dots & f(\zeta_n)\zeta_n \\ \cdot & \cdot & \cdot & \cdot \\ f(\zeta_1)\zeta_1^{n-2} & f(\zeta_2)\zeta_2^{n-2} & \dots & f(\zeta_n)\zeta_n^{n-2} \end{vmatrix} \left[\prod_{k=1}^{n} \zeta_k \right]^{1-n} =$$

$$= \left[\prod_{k=1}^{n} \zeta_k \right]^{1-n} \left[\prod_{k=1}^{n} f(\zeta_k) \right] V(-1)^{n-1}.$$

Kako su ζ_k koreni jednačine $x^n - 1 = 0$, to je

$$\prod_{k=1}^{n} \zeta_k = (-1)^{n+1},$$

pa izlazi

$$D = (-1)^{n-n^2} \prod_{k=1}^{n} f(\zeta_k) = \prod_{k=1}^{n} f(\zeta_k),$$

što je i trebalo dokazati.

Lema 2.2 Za kosocikličku determinantu

$$D = \begin{vmatrix} a_1 & a_2 & a_3 & \dots & a_n \\ -a_n & a_1 & a_2 & \dots & a_{n-1} \\ -a_{n-1} & -a_n & a_1 & \dots & a_{n-2} \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ -a_2 & -a_3 & -a_4 & \dots & a_1 \end{vmatrix} \qquad (2.13)$$

važi

$$D = \prod_{k=1}^{n} f(\zeta_k), \qquad (2.14)$$

gde je $\zeta_k = \sqrt[n]{-1} = \cos\frac{(2k-1)\pi}{n} + i\sin\frac{(2k-1)\pi}{n}$, $k = 1, 2, \dots n$,

$f(x) = a_1 + a_2 x + \dots + a_n x^{n-1}$.

Dokaz. Analogno dokazu leme 2.1, množeći determinantu D sa determinantom Vandermond-a, čiju su elementi ζ_k sve vrednosti

n-tog korena iz -1, pa množeći zatim prvu kolonu dobijene determinante sa ζ_1^{n-1}, drugu sa ζ_2^{n-1},..., n-tu sa ζ_n^{n-1} i vodeći računa da je $\zeta_k^n = -1$ za svako $k=1,2,...n$, dobijamo

$$DV = \left[\prod_{k=1}^{n} \zeta_k\right]^{1-n} \begin{vmatrix} f(\zeta_1)\zeta_1^{n-1} & f(\zeta_2)\zeta_2^{n-1} \ldots & f(\zeta_n)\zeta_n^{n-1} \\ -f(\zeta_1) & -f(\zeta_2) \ldots & -f(\zeta_n) \\ -f(\zeta_1)\zeta_1 & -f(\zeta_2)\zeta_2 \ldots & -f(\zeta_n)\zeta_n \\ \cdot \quad \cdot \quad \cdot & \cdot \quad \cdot \quad \cdot & \cdot \quad \cdot \quad \cdot \\ -f(\zeta_1)\zeta_1^{n-2} & -f(\zeta_2)\zeta_2^{n-2} \ldots & -f(\zeta_n)\zeta_n^{n-2} \end{vmatrix} =$$

$$= (-1)^{n-1} \prod_{k=1}^{n} f(\zeta_k) \left[\prod_{k=1}^{n} \zeta_k\right]^{1-n} (-1)^{n-1} V.$$

Kako su ζ_k koreni jednačine $x^n + 1 = 0$, to je

$$\prod_{k=1}^{n} \zeta_k = (-1)^n,$$

pa izlazi

$$D = (-1)^{n(1-n)} \prod_{k=1}^{n} f(\zeta_k) = \prod_{k=1}^{n} f(\zeta_k),$$

što je i trebalo dokazati.

Na osnovu prethodne dve leme sada nije teško izračunati determinante odredjene definicijama 2.1-2.3.

Lema 2.3 Važi jednakost

$$A_{n,r} = \prod_{k=1}^{\frac{n-1}{2}} \left(1 + 8\cos\frac{k\pi}{n}\sin\frac{k(r-1)\pi}{n}\sin\frac{kr\pi}{n}\right) \qquad (2.15)$$

Dokaz. Prema (2.7) determinanta $A_{n,r}$ je oblika (2.11), pri čemu je $f(x) = -1 + x^{n-r} - x^{n-1}$. Na osnovu leme 2.1 biće

$$A_{n,r} = -\prod_{k=1}^{n} (-1 + \zeta_k^{n-r} - \zeta_k^{n-1}),$$

gde su ζ_k sve vrednosti $\sqrt[n]{1}$. Neka je $\zeta = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$, tada su $\zeta, \zeta^2, \ldots \zeta^{n-1}$, 1, sve vrednosti $\sqrt[n]{1}$. Sledi

$$A_{n,r} = \prod_{k=1}^{n-1} (-1 + \zeta^{k(n-r)} - \zeta^{k(n-1)}). \qquad (2.16)$$

Množeći svaki od faktora u (2.16) redom sa ζ^k, $k=1,2,\ldots n-1$, dobijamo

$$A_{n,r} = \left[\prod_{k=1}^{n-1} \zeta^k\right]^{-1} \prod_{k=1}^{n-1} (-1 - \zeta^k + \zeta^{k(n-r+1)}) =$$

$$= \prod_{k=1}^{\frac{n-1}{2}} (-1 - \zeta^k + \zeta^{k(n-r+1)})(-1 - \zeta^{n-k} + \zeta^{(n-k)(n-r+1)}) =$$

$$= \prod_{k=1}^{\frac{n-1}{2}} (3 + \zeta^k + \zeta^{-k} - \zeta^{k(n-r+1)} - \zeta^{-k(n-r+1)} - \zeta^{k(n-r)} -$$

$$- \zeta^{-k(n-r)}).$$

Kako je $\zeta^{-s} = \cos\frac{2s\pi}{n} - i\sin\frac{2s\pi}{n} = \overline{\zeta}^s$, gde je $\overline{\zeta}^s$ konjugovano kompleksan broj broju ζ^s, to poslednja jednakost daje

$$A_{n,r} = \prod_{k=1}^{\frac{n-1}{2}} (3 + 2\cos\frac{2k\pi}{n} - 2\cos\frac{2k(n-r+1)\pi}{n} -$$

$$- 2\cos\frac{2k(n-r)\pi}{n}) = \prod_{k=1}^{\frac{n-1}{2}} (1 + 8\cos\frac{k\pi}{n}\sin\frac{k(n-r+1)\pi}{n}\sin\frac{k(n-r)\pi}{n}) =$$

$$= \prod_{k=1}^{\frac{n-1}{2}} (1 + 8\cos\frac{k\pi}{n}\sin\frac{k(r-1)\pi}{n}\sin\frac{kr\pi}{n}),$$

što je i trebalo dokazati.

Lema 2.4 Važi jednakost

$$C_{n,r} = \prod_{k=1}^{\frac{n-1}{2}} (1 + 8\cos\frac{k\pi}{n}\cos\frac{k(r-1)\pi}{n}\cos\frac{kr\pi}{n})$$

Dokaz. Prema (2.8) determinanta $C_{n,r}$ je oblika (2.11), pri čemu

je $f(x) = 1 + x^{n-r} + x^{n-1}$. Na osnovu leme 2.1 rezonujući slično kao u dokazu leme 2.3 dobijamo

$$C_{n,r} = \frac{1}{3} \prod_{k=1}^{n} (1 + \zeta_k^{n-r} + \zeta_k^{n-1}) = \frac{1}{3} \prod_{k=1}^{n} (1 + \zeta^{k(n-r)} +$$

$$+ \zeta^{k(n-1)}) = \left[\prod_{k=1}^{n-1} \zeta^k\right]^{-1} \prod_{k=1}^{n-1} (1 + \zeta^k + \zeta^{k(n-r+1)}) =$$

$$= \prod_{k=1}^{\frac{n-1}{2}} (1 + \zeta^k + \zeta^{k(n-r+1)})(1 + \zeta^{n-k} + \zeta^{(n-k)(n-r+1)}) =$$

$$= \prod_{k=1}^{\frac{n-1}{2}} (3 + 2\cos\frac{2k\pi}{n} + 2\cos\frac{2k(n-r+1)\pi}{n} + 2\cos\frac{2k(n-r)\pi}{n}) =$$

$$= \prod_{k=1}^{\frac{n-1}{2}} (1 + 8\cos\frac{k\pi}{n}\cos\frac{k(r-1)\pi}{n}\cos\frac{kr\pi}{n}),$$

što je i trebalo dokazati.

Lema 2.5 Važi jednakost

$$B_{m,n,r} = \prod_{k=1}^{2^{m-2}n} (1 + 8\cos\frac{(2k-1)\pi}{2^m n}\sin\frac{(2k-1)(r-1)\pi}{2^m n}\sin\frac{(2k-1)r\pi}{2^m n}). \qquad (2.18)$$

Dokaz. Prema definiciji 2.2 moramo razlikovati dva slučaja: $r=3,5,\ldots,2^{m-1}n-3$ i $r=2^{m-1}n+3, 2^{m-1}n+5,\ldots,2^m n-1$. U oba slučaja $B_{m,n,r}$ je oblika (2.13), pri čemu je u prvom slučaju

$$f(x) = -1 - x^{2^{m-1}n-r} + x^{2^{m-1}n-1}, \qquad (2.19)$$

a u drugom

$$f(x) = -1 + x^{2^m n-r} + x^{2^{m-1}n-1}. \qquad (2.20)$$

Neka su ζ_k, $k=1,2,\ldots 2^{m-1}n$, sve vrednosti $2^{m-1}n$-tog korena iz -1. Tada je

$$\zeta_k = \cos\frac{(2k-1)\pi}{2^{m-1}n} + i\sin\frac{(2k-1)\pi}{2^{m-1}n} = (\cos\frac{2\pi}{2^m n} + i\sin\frac{2\pi}{2^m n})^{2k-1} = \mu^{2k-1}. \qquad (2.21)$$

Očigledno važi

$$\mu^{2^{m-1}n} = -1, \quad \mu^{(2^{m-1}n)^2} = 1. \tag{2.22}$$

Uzimajući u obzir (2.19), (2.21) i (2.22), na osnovu leme 2.2 u prvom slučaju dobijamo

$$B_{m,n,r} = \prod_{k=1}^{2^{m-1}n} (-1 - \zeta_k^{2^{m-1}n-r} + \zeta_k^{2^{m-1}n-1}) =$$

$$= \prod_{k=1}^{2^{m-1}n} (-1 - \mu^{(2k-1)(2^{m-1}n-r)} + \mu^{(2k-1)(2^{m-1}n-1)}) =$$

$$= \left[\prod_{k=1}^{2^{m-1}n} \mu^{2k-1}\right]^{-1} \prod_{k=1}^{2^{m-1}n} (-1 - \mu^{2k-1} - \mu^{(2k-1)(2^{m-1}n-r+1)}) =$$

$$= \mu^{-(2^{m-1}n)^2} \prod_{k=1}^{2^{m-1}n} (-1 - \mu^{2k-1} + \mu^{(2k-1)(1-r)}) =$$

$$= \prod_{k=1}^{2^{m-2}n} (-1 - \mu^{2k-1} + \mu^{(2k-1)(1-r)})(-1 - \mu^{2^m n-2k+1} + \mu^{(2^m n-2k+1)(1-r)}) =$$

$$= \prod_{k=1}^{2^{m-2}n} (3 + \mu^{2k-1} + \overline{\mu}^{2k-1} - \mu^{(2k-1)(1-r)} - \overline{\mu}^{(2k-1)(1-r)} - \mu^{-(2k-1)r} -$$

$$- \overline{\mu}^{-(2k-1)r}) = \prod_{k=1}^{2^{m-2}n} (3 + 2\cos\frac{2(2k-1)\pi}{2^m n} - 2\cos\frac{2(2k-1)(r-1)\pi}{2^m n} -$$

$$- 2\cos\frac{2(2k-1)r\pi}{2^m n}) = \prod_{k=1}^{2^{m-2}n} (1 +$$

$$+ 8\cos\frac{(2k-1)\pi}{2^m n}\sin\frac{(2k-1)(r-1)\pi}{2^m n}\sin\frac{(2k-1)r\pi}{2^m n}).$$

Uzimajući u obzir (2.20), (2.21) i (2.22), na osnovu leme 2.2, u drugom slučaju analogno se dobija

$$B_{m,n,r} = \prod_{k=1}^{2^{m-1}n} (-1 + \zeta_k^{2^m n-r} + \zeta_k^{2^{m-1}n-1}) =$$

$$= \prod_{k=1}^{2^{m-1}n} (-1 + \mu^{(2k-1)(2^m n-r)} + \mu^{(2k-1)(2^{m-1}n-1)}) =$$

$$= \left[\prod_{k=1}^{2^{m-1}n} \mu^{2k-1}\right]^{-1} \prod_{k=1}^{2^{m-1}n} (-1 - \mu^{2k-1} + \mu^{(2k-1)(2^m n-r+1)}) =$$

$$= \prod_{k=1}^{2^{m-1}n} (-1 - \mu^{2k-1} + \mu^{(2k-1)(1-r)}) =$$

$$= \prod_{k=1}^{2^{m-2}n} (1 + 8\cos\frac{(2k-1)\pi}{2^m n} \sin\frac{(2k-1)r\pi}{2^m n} \sin\frac{(2k-1)(r-1)\pi}{2^m n}).$$

Time je lema u potpunosti dokazana.

Primetimo da su rezultati dobijeni u prethodne tri leme i sami za sebe interesantni. U jednakostima (2.15), (2.16) i (2.17) s leve strane stoje determinante, čiji su rezultati evidentno celi brojevi, a s desne strane konačni proizvodi čiji su faktori iracionalni. Primetimo dalje, što za nas može biti vrlo značajno, da dobijeni rezultati dozvoljavaju efikasnu primenu računara na izračunavanje pomenutih determinanti. Naime, dobijeni proizvodi se vrlo lako mogu izračunati sa greškom manjom od 10^{-1}.

Preostalo je da se još izračuna $D_{m,n,r}$.

Lema 2.6 Važi jednakost

$$D_{m,n,r} = \prod_{k=1}^{2^{m-1}} \left[\sum_{i=o}^{2^{m-1}-1} a_i \mu^{(2k-1)(2^{m-1}-i)}\right], \qquad (2.23)$$

gde je $\mu = \cos\frac{2\pi}{2^m} + i\sin\frac{2\pi}{2^m}$. Specijalno, za $m=3$

$$D_{3,n,r} = (a_o^2 - a_2^2 + 2a_1a_3)^2 + (a_1^2 - a_3^2 - 2a_oa_2)^2. \qquad (2.24)$$

Dokaz. Determinanta $D_{m,n,r}$ je oblika (2.13), pa na osnovu leme 2.2 dobijamo

$$D_{m,n,r} = \prod_{k=1}^{2^{m-1}} \left[a_o - \sum_{i=1}^{2^{m-1}-1} a_i \zeta_k^{2^{m-1}-i} \right],$$

gde su ζ_k, $k=1,2,\ldots 2^{m-1}$ sve vrednosti 2^{m-1}-og korena iz -1. Kako je

$$\zeta_k = \cos\frac{(2k-1)\pi}{2^{m-1}} + i\sin\frac{(2k-1)\pi}{2^{m-1}} = \left(\cos\frac{2\pi}{2^m} + i\sin\frac{2\pi}{2^m}\right)^{2k-1} = \mu^{2k-1},$$

to sledi

$$D_{m,n,r} = \prod_{k=1}^{2^{m-1}} \left[a_o - \sum_{i=1}^{2^{m-1}-1} a_i \mu^{(2k-1)(2^{m-1}-i)} \right] =$$

$$= \prod_{k=1}^{2^{m-1}} \left[\sum_{i=o}^{2^{m-1}-1} a_i \mu^{(2k-1)(2^{m-1}-i)} \right],$$

što je i trebalo dokazati.

Za $m=3$, $\mu = \cos\frac{\pi}{4} + i\sin\frac{\pi}{4} = \frac{\sqrt{2}}{2}(1+i)$, $\mu^2 = i$, $\mu^3 = \frac{\sqrt{2}}{2}(-1+i)$, pa (2.23) neposredno daje (2.24).

2.3 Par kongruencija $(t+1)^s \equiv t^s \equiv 1 \pmod q$

Sada smo u stanju da pristupimo razmatranju kongruencija (2.2). Ograničićemo se na slučaj kada je $s=2^m n$, gde je $m \in N$, a $n=1$ ili $n \in P$, $n \geq 5$. S druge strane, posmatraćemo malo širi slučaj kada je $q=2^k np+1$, gde je $k \in N$, u krajnjoj liniji, nezavisan od m. Dakle, razmatramo problem: pod kojim uslovima kongruencije

$$(t+1)^{2^m n} \equiv 1 \pmod q,\ t^{2^m n} \equiv 1 \pmod q,\ q=2^k np+1 \in P \quad (2.25)$$

imaju zajedničko rešenje. Jasno je da će, s obzirom na teoremu 2.1, nas posebno interesovati specijalan slučaj $k=m$.

Pre nego što iskažemo i dokažemo teoremu koja će odgovoriti na pitanje postavljeno u vezi sa kongruencijama (2.25), utvrdimo nekoliko elementarnih činjenica i uvedimo nekoliko pojmova.

Nije teško pokazati da ako je D rezultanta polinoma $P(t)$ i $Q(t)$, da će iz činjenice da kongruencije

$$P(t) \equiv o \pmod q, \quad Q(t) \equiv o \pmod q \tag{2.26}$$

imaju zajedničko rešenje, slediti da mora biti

$$D \equiv o \pmod q.$$

Naime, ako kongruencije (2.26) imaju zajedničko rešenje, tada postoje $k_1, k_2 \in D$, takvi da jednačine

$$P(t) - k_1 q = o, \quad Q(t) - k_2 q = o$$

imaju zajedničko rešenje. Tvrdjenje sledi iz

$$D \equiv D_1 \pmod q,$$

gde je D_1 rezultanta polinoma $P(t) - k_1 q$ i $Q(t) - k_2 q$.

Primetimo da obrnuto tvrdjenje u opštem slučaju ne važi. Na primer, kongruencija $t^2 + 1 \equiv o \pmod 7$ nema rešenja, pa ni kongruencije $t^4 \equiv 1$, $t^2 \equiv -1 \pmod 7$ nemaju zajedničko rešenje. Medjutim, za rezultantu D polinoma $t^4 - 1$, $t^2 + 1$ očigledno važi $D=0$, pa je $D \equiv 0 \pmod 7$.

Neka je $n \in P$, $n \geq 5$, i neka je $3 \leq r \leq n-2$, $r \neq \frac{n+1}{2}$. U skup svih takvih r uvedimo relaciju ρ definisanu sa

$$r \rho r_1 \Leftrightarrow r_1 \in \{1-r, \frac{1}{r}, 1 - \frac{1}{r}, \frac{1}{1-r}, \frac{r}{r-1}\},$$

gde su elementi gornjeg skupa uzeti po modulu n. Relacija ρ je očigledno simetrična, pa razbija polazni skup svih uočenih r na uniju disjunktnih podskupova. Svaki takav podskup ima šest elemenata, ako medju brojevima r, $1-r$, $\frac{1}{r}$, $1 - \frac{1}{r}$, $\frac{1}{1-r}$, $\frac{r}{r-1}$ nema kongruentnih po modulu n. Kako je $r \neq 1, 2, -1, \frac{n+1}{2}$, to je $r \rho r$ ako i samo ako važi $r^2 - r + 1 \equiv o \pmod n$. Prema lemi 1.5 poslednja kongruencija ima dva rešenja ako i samo ako je $n = 2 \cdot 3\lambda + 1$.

Dakle, relacija ρ je razbila polazni skup na uniju disjunktnih podskupova, od kojih svaki ima po šest elemenata, izuzev eventualno jednog, u slučaju $n = 6\lambda + 1$, koji ima dva elementa. Neka je S skup svih predstavnika ovih disjunktnih podskupova, birajući za predstavnika najmanji r.

Primetimo da, bez obzira da li je $n = 6\lambda + 1$ ili $n = 6\lambda + 5$, skup S ima uvek λ elemenata. Znači, u svakom slučaju, skup S ima $[\frac{n-1}{6}]$ elemenata.

Definicija 2.4 Neka je $n=1$ ili $n \in P$, $n \geq 5$. Pod A_n i C_n podrazumevaćemo sledeće

$$A_n = \begin{cases} 1, & n=1 \\ \prod_{r=2}^{\frac{n-1}{2}} A_{n,r}, & n \in P,\ n \geq 5 \end{cases}, \tag{2.27}$$

$$C_n = \begin{cases} 1, & n=1,\ 5 \\ \prod_{r \in S} C_{n,r}, & n \in P,\ n \geq 7 \end{cases}. \tag{2.28}$$

Definicija 2.5 Neka je $m \in N$, $n=1$ ili $n \in P$, $n \geq 5$. Neka je dalje $S_3 = \{3, 5, \ldots 2^{m-1}n-3,\ 2^{m-1}n+3, \ldots 2^m n-1\}$ i neka je

$$S_1 = S_3 \setminus \{r_1 : r, r_1 \in S_3 \wedge r_1 > r \wedge rr_1 \equiv 1 \pmod{2^m n}\}.$$

Pod $B_{m,n}$ podrazumevaćemo sledeće

$$B_{m,n} = \begin{cases} 1, & m=1 \vee m=2,\ n=1 \\ \prod_{i=2}^{m} \left[\prod_{r \in S_1} B_{i,n,r} \right], & m \geq 3 \vee m=2,\ n \geq 5 \end{cases}. \tag{2.29}$$

Definicija 2.6 Neka je $m \in N$, $n=1$ ili $n \in P$, $n \geq 5$. Neka je dalje

$$S_2 = \{1, 3, \ldots 2^{m-1}-1\}.$$

Pod $D_{m,n}$ podrazumevaćemo sledeće

$$D_{m,n} = \begin{cases} 1, & 1 \leq m \leq 2 \vee n=1 \\ \prod_{i=3}^{m} \left[\prod_{r \in S_2} D_{i,n,r} \right], & m \geq 3 \wedge n \in P,\ n \geq 5 \end{cases}. \tag{2.30}$$

Dokažimo konačno sledeću teoremu.

Teorema 2.2 Neka je $m \in N$, $n=1$ ili $n \in P$, $n \geq 5$, $q = 2^k np+1 \in P$, $k \in N$, $p \in P$, $p \geq 5$. Ako važi

$$A_n B_{m,n} C_n D_{m,n} (2^{2^m n} - 1) \not\equiv 0 \pmod{q}, \tag{2.31}$$

tada kongruencije

$$(t+1)^{2^m n} \equiv 1 \pmod{q}, \quad t^{2^m n} \equiv 1 \pmod{q} \tag{2.32}$$

nemaju zajedničko rešenje.

Dokaz. Izvedimo dokaz matematičkom indukcijom po m. Za $m=1$ uslov (2.31) postaje

$$\Lambda_n C_n (2^{2n} - 1) \not\equiv 0 \pmod{q}. \qquad (2.33)$$

Pretpostavimo obrnuto, neka važi (2.33) i neka kongruencije (2.32) imaju zajedničko rešenje. Pre svega, mora biti $n \geqslant 5$. Stvarno, za $n=1$, uslov (2.33) daje $2^2 - 1 = 3 \not\equiv 0 \pmod{q}$ za svako $q = 2^k p + 1$. S druge strane, iz $(t+1)^2 \equiv 1$, $t^2 \equiv 1 \pmod{q}$ izlazi $2^2 \equiv 1 \pmod{q}$, što je nemoguće, pa je za $m=n=1$ tvrdjenje teoreme tačno.

Neka je dakle, $m=1$, $n \geqslant 5$. Kongruencije (2.32) ekvivalentne su sledećim kongruencijama

$$t^n \equiv 1 \pmod{q} \quad (t+1)^n \equiv 1 \pmod{q}, \qquad (2.34)$$

$$t^n \equiv 1 \pmod{q} \quad (t+1)^n \equiv -1 \pmod{q}, \qquad (2.35)$$

$$t^n \equiv -1 \pmod{q} \quad (t+1)^n \equiv 1 \pmod{q}, \qquad (2.36)$$

$$t^n \equiv -1 \pmod{q} \quad (t+1)^n \equiv -1 \pmod{q}. \qquad (2.37)$$

Stavljajući u (2.37) $t \equiv -1-z \pmod{q}$ izlazi

$$-1 \equiv t^n \equiv (-1-z)^n = -(1+z)^n \pmod{q} \Rightarrow (z+1)^n \equiv 1 \pmod{q},$$

$$-1 \equiv (t+1)^n \equiv (-z)^n = -z^n \pmod{q} \Rightarrow z^n \equiv 1 \pmod{q}.$$

Znači, kongruencije (2.37) se svode na kongruencije (2.34). Takodje, stavljajući u (2.36) $t \equiv -1 - \frac{1}{z} \pmod{q}$ izlazi

$$-1 \equiv t^n \equiv (-1 - \frac{1}{z})^n = -\frac{(z+1)^n}{z^n} \pmod{q} \Rightarrow z^n \equiv (z+1)^n \pmod{q},$$

$$1 \equiv (t+1)^n \equiv (-\frac{1}{z})^n = -\frac{1}{z^n} \pmod{q} \Rightarrow z^n \equiv -1 \pmod{q},$$

pa se kongruencije (2.36) svode na kongruencije (2.37), a preko njih, na kongruencije (2.34).

Dakle, kongruencije (2.32) za $m=1$, $n \geqslant 5$, imaju zajedničko rešenje, ako i samo ako bar jedne od kongruencija (2.34), (2.35) imaju zajedničko rešenje. Razmotrimo oba slučaja.

Neka kongruencije (2.34) imaju zajedničko rešenje.Zbog uslova $2^{2n} - 1 \not\equiv 0 \pmod{q}$, mora biti $t \not\equiv 1 \pmod{q}$. No, onda postoji r takav, da je $t^r \equiv t+1 \pmod{q}$, $2 \leqslant r \leqslant n-1$. Znači, kongruencije

$$t^n \equiv 1 \pmod{q}, \quad t^r \equiv t+1 \pmod{q} \qquad (2.38)$$

imaju zajedničko rešenje.

Stavljajući u (2.38) $t \equiv \frac{1}{z} \pmod{q}$ izlazi

$$z^n \equiv 1 \pmod q, \quad z^{1-r} \equiv z+1 \pmod q.$$

Sledi, ako kongruencije (2.38) imaju zajedničko rešenje za neko r, tada one imaju zajedničko rešenje za $1-r \pmod n$. Znači, možemo uzeti $2 \leqslant r \leqslant \frac{n+1}{2}$. Za $r = \frac{n+1}{2}$ (2.38) daje

$$(t+1)^2 \equiv t^{n+1} \equiv t \pmod q \Rightarrow t^2+t+1 \equiv 0 \pmod q.$$

Prema lemi 1.5, mora biti $q=6\lambda+1$, tj. $2^{k-1}np=3\lambda$, što je nemoguće, jer je $2^{k-1}np \not\equiv 0 \pmod 3$. Dakle, konačno $2 \leqslant r \leqslant \frac{n-1}{2}$.

Neka je D rezultanta polinoma t^n-1 i t^r-t-1. Kako po pretpostavci kongruencije (2.38) imaju zajedničko rešenje, to mora biti

$$D \equiv 0 \pmod q. \qquad (2.39)$$

Odredimo rezultantu D. Imamo

$$D = \begin{vmatrix} 1 & 0 & 0 & \dots & 0 & -1 & 0 & \dots & 0 & 0 \\ 0 & 1 & 0 & \dots & 0 & 0 & -1 & \dots & 0 & 0 \\ \dots & & & & & & & & & \\ 0 & 0 & 0 & \dots & 1 & 0 & 0 & \dots & 0 & -1 \\ 1 & 0 & 0 & \dots & -1 & -1 & 0 & \dots & 0 & 0 \\ 0 & 1 & 0 & \dots & 0 & -1 & -1 & \dots & 0 & 0 \\ \dots & & & & & & & & & \\ 0 & 0 & 0 & \dots & 1 & 0 & 0 & \dots & -1 & -1 \end{vmatrix}$$

($n+1$-va kolona; r vrsta; n vrsta)

Determinanta D je $n+r$-tog reda, pri čemu imajmo na umu da je $2 \leqslant r \leqslant \frac{n-1}{2}$. Dodamo li prvu kolonu $n+1$-voj, drugu $n+2$-goj, ..., r-tu $n+r$-toj, razvijajući potom determinantu po prvih r vrsta, dobijamo

$$D = \begin{vmatrix} -1 & & & 1 & & -1 \\ -1 & \ddots & & & \ddots & \\ & \ddots & & & \ddots & 0 \\ & & 0 & & & 1 \\ 1 & \cdots & & \cdots & & \\ & \ddots & 0 & & & \\ 0 & & 1 & & -1 & -1 \end{vmatrix} = -A_{n,r}.$$

Iz (2.39) sledi da za neko r $2 \leqslant r \leqslant \frac{n-1}{2}$ važi $A_{n,r} \equiv 0 \pmod q$. No, onda je $A_n \equiv 0 \pmod q$, što protivreči sa uslovom (2.33).

Dakle, kongruencije (2.38), pa dakle i kongruencije (2.34),(2.36), (2.37) nemaju zajedničko rešenje.

Preostalo je da kongruencije (2.35) moraju da imaju zajedničko rešenje. Zbog uslova $2^{2n}-1 \not\equiv 0 \pmod q$, mora biti $t \not\equiv 1 \pmod q$. No, onda postoji r takav da je $t^r \equiv -t-1 \pmod q$, $2 \leqslant r \leqslant n-1$. Znači, kongruencije

$$t^n \equiv 1 \pmod q, \quad t^r \equiv -t-1 \pmod q \tag{2.40}$$

imaju zajedničko rešenje.

Za $r=2$, $r=n-1$, (2.40) daje $t^2+t+1 \equiv 0 \pmod q$, pa prema lemi 1.5 mora biti $q=6\lambda+1$, tj. $2^{k-1}pn=3\lambda$, što je nemoguće. Takodje, za $r = \frac{n+1}{2}$, (2.40) daje

$$(t+1)^2 \equiv t^{n+1} \equiv t \pmod q \Rightarrow t^2+t+1 \equiv 0 \pmod q,$$

što je, videli smo, nemoguće. Znači, $3 \leqslant r \leqslant n-2$, $r \neq \frac{n+1}{2}$.

Stavljajući u (2.40) $t \equiv \frac{1}{z} \pmod q$ izlazi

$$z^n \equiv 1 \pmod q, \quad z^{1-r} \equiv -z-1 \pmod q.$$

Takodje, stavljajući u (2.40) $t \equiv -1-z \pmod q$ izlazi

$$(z+1)^n \equiv -1 \pmod q, \quad -t-1 \equiv z \equiv (-1-z)^r \pmod q,$$

odnosno, za $rr_1 \equiv 1 \pmod n$,

$$z^{r_1} \equiv (-1-z)^{rr_1} \equiv -1-z \pmod q, \quad z^n \equiv (-1-z)^{nr} \equiv 1 \pmod q.$$

Znači, ako za neko r, $3 \leqslant r \leqslant n-2$, $r \neq \frac{n+1}{2}$, kongruencije (2.40) imaju zajedničko rešenje, tada one imaju zajedničko rešenje i za $1-r$, $\frac{1}{r}$, $1-\frac{1}{r}$, $\frac{1}{1-r}$, $\frac{r}{r-1}$, gde su uzete vrednosti po modulu n. Drugim rečima, kongruencije (2.40) imaju zajedničko rešenje za neko $r \in S$, gde je S skup, kojeg smo ranije definisali.

Ako sa D' označimo rezultantu polinoma t^n-1 i t^r+t+1, mora biti

$$D' \equiv 0 \pmod q. \tag{2.41}$$

Izračunavajući determinantu D' analogno kao determinantu D, dobijamo

$$D' = \begin{vmatrix} 1 & 0 & 0 & \dots & 0 & -1 & 0 & \dots & 0 & 0 \\ 0 & 1 & 0 & \dots & 0 & 0 & -1 & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 1 & 0 & 0 & \dots & 0 & -1 \\ 1 & 0 & 0 & \dots & 1 & 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & 0 & \dots & 0 & 1 & 1 & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 1 & 0 & 0 & \dots & 1 & 1 \end{vmatrix} =$$

$$= \begin{vmatrix} 1 & & & & 1 \\ 1 & \ddots & & \iddots & \\ & & \mathbf{0} & & 1 \\ 1 & \iddots & & \ddots & \\ & & & & \\ \mathbf{0} & & 1 & & 1 \end{vmatrix} = 3C_{n,r}.$$

Iz (2.41) sledi da za neko $r \in S$ važi $3C_{n,r} \equiv 0 \pmod q$, tj. $C_{n,r} \equiv 0 \pmod q$. No, onda je $C_n \equiv 0 \pmod q$, što protivreči sa uslovom (2.33). Dakle, kongruencije (2.40), pa dakle i kongruencije (2.35) nemaju zajedničko rešenje. Time je za $m=1$ teorema u potpunosti dokazana.

Pretpostavimo da je tvrdjenje teoreme tačno za neki prirodan broj $m-1$ i dokažimo da je tvrdjenje tačno za prirodan broj $m \geqslant 2$. Pretpostavimo obrnuto, neka važi (2.31) i neka kongruencije (2.32) imaju zajedničko rešenje.

Kongruencije (2.32) su ekvivalentne kongruencijama

$$t^{2^{m-1}n} \equiv 1 \pmod q, \quad (t+1)^{2^{m-1}n} \equiv 1 \pmod q, \tag{2.42}$$

$$t^{2^{m-1}n} \equiv 1 \pmod q, \quad (t+1)^{2^{m-1}n} \equiv -1 \pmod q, \tag{2.43}$$

$$t^{2^{m-1}n} \equiv -1 \pmod q, \quad (t+1)^{2^{m-1}n} \equiv 1 \pmod q, \tag{2.44}$$

$$t^{2^{m-1}n} \equiv -1 \pmod q, \quad (t+1)^{2^{m-1}n} \equiv -1 \pmod q. \tag{2.45}$$

Stavljajući u (2.43) $t \equiv -1-z \pmod q$ izlazi

$$1 \equiv t^{2^{m-1}n} \equiv (-1-z)^{2^{m-1}n} = (1+z)^{2^{m-1}n} \pmod q,$$

$$-1 \equiv (t+1)^{2^{m-1}n} \equiv (-z)^{2^{m-1}n} = z^{2^{m-1}n} \pmod q.$$

Takodje, stavljajući u (2.44) $t \equiv -\frac{1}{1+z} \pmod q$ izlazi

$$-1 \equiv t^{2^{m-1}n} \equiv (\frac{1}{1+z})^{2^{m-1}n} \pmod q \Rightarrow (1+z)^{2^{m-1}n} \equiv -1 \pmod q,$$

$$1 \equiv (t+1)^{2^{m-1}n} \equiv (\frac{z}{z+1})^{2^{m-1}n} \pmod q \Rightarrow z^{2^{m-1}n} \equiv -1 \pmod q.$$

Znači, kongruencije (2.43) se svode na kongruencije (2.44), a ove pak, na kongruencije (2.45). Sledi, ako kongruencije (2.32) imaju zajedničko rešenje, tada bar jedan par kongruencija (2.42), odnosno (2.45) ima zajedničko rešenje.

Kako je

$$A_n B_{m,n} C_n D_{m,n} (2^{2^m n} - 1) =$$

$$= A_n C_n (2^{2^{m-1}n} - 1)(2^{2^{m-1}n} + 1) B_{m-1,n} \Big[\prod_{r \in S_1} B_{m,n,r}\Big] D_{m-1,n} \Big[\prod_{r \in S_2} D_{m,n,r}\Big] =$$

$$= M A_n C_n (2^{2^{m-1}n} - 1) B_{m-1,n} D_{m-1,r'}$$

to iz uslova (2.31) sledi

$$A_n C_n B_{m-1,n} D_{m-1,n} (2^{2^{m-1}n} - 1) \not\equiv 0 \pmod q,$$

pa je ispunjen uslov teoreme za prirodan broj $m-1$, te po induktivnoj pretpostavci kongruencije (2.42) nemaju zajedničko rešenje. Preostaje da kongruencije (2.45) moraju imati zajedničko rešenje.

Pretpostavimo prvo, da važi

$$t^{2^{m-1}} \not\equiv -1 \pmod q. \qquad (2.46)$$

Sledi, postoji neparan broj r, $3 \leqslant r \leqslant 2^m n-1$, takav da je $t^r \equiv t + 1 \pmod q$. Znači, kongruencije

$$t^{2^{m-1}n} \equiv -1 \pmod q, \quad t^r \equiv t+1 \pmod q \qquad (2.47)$$

imaju zajedničko rešenje. Stavljajući u (2.47) $t \equiv -1-z \pmod q$ izlazi

$$t^r \equiv (-1-z)^r = -(1+z)^r \equiv t+1 \equiv -z \pmod q \Rightarrow (1+z)^r \equiv z \pmod q.$$

Ako postoji r_1 takvo da je $rr_1 \equiv 1 \pmod{2^m n}$, sledi

$$z^{r_1} \equiv (1+z)^{rr_1} = (1+z)^{2^m n\lambda + 1} = (-1-z)^{2^m n\lambda}(1+z) \equiv$$

$$\equiv (t^{2^{m-1}n})^{2\lambda}(1+z) \equiv (-1)^{2\lambda}(1+z) \equiv 1+z \pmod q.$$

Znači, ako za neko r, $3\leqslant r\leqslant 2^m n-1$, kongruencije (2.47) imaju zajedničko rešenje, onda one imaju zajedničko rešenje i za r_1, $3\leqslant r_1\leqslant 2^m n-1$, $rr_1\equiv 1 \pmod{2^m n}$. Kako za $r=2^{m-1}n+1$ (2.47) daje

$$2t \equiv -1 \pmod q \Rightarrow 2^{2^{m-1}n} \equiv 1 \pmod q,$$

što protivreči uslovu (2.31), a za $r=2^{m-1}n-1$ (2.47) daje

$$t^2+t+1 \equiv 0 \pmod q \Rightarrow q=6\lambda+1 \Rightarrow 2^{k-1}np=3\lambda,$$

što je nemoguće, to kongruencije (2.47) imaju zajedničko rešenje za neko $r\in S_1$, gde je S_1 odredjen u definiciji 2.5.

Znači, postoji $r\in S_1$ takvo da je

$$R \equiv 0 \pmod q, \tag{2.48}$$

gde je R rezultanta polinoma $t^{2^{m-1}n}+1$ i t^r-t-1. Izračunajmo determinantu R. Razlikovaćemo dva slučaja: $3\leqslant r\leqslant 2^{m-1}n-3$ i $2^{m-1}n+3\leqslant r\leqslant 2^m n-1$. U prvom slučaju je

$$R=\begin{vmatrix} 1 & 0 & 0 & \dots & 0 & 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & 0 & \dots & 0 & 0 & 1 & \dots & 0 & 0 \\ \dots & & & & & & & & & \\ 0 & 0 & 0 & \dots & 1 & 0 & 0 & \dots & 0 & 1 \\ 1 & 0 & 0 & \dots & -1 & -1 & 0 & \dots & 0 & 0 \\ 0 & 1 & 0 & \dots & 0 & -1 & -1 & \dots & 0 & 0 \\ \dots & & & & & & & & & \\ 0 & 0 & 0 & \dots & 1 & 0 & 0 & \dots & -1 & -1 \end{vmatrix} \begin{matrix} r \text{ vrsta} \\ \\ \\ \\ 2^{m-1}n \text{ vrsta} \\ \\ \\ \end{matrix}$$

Ako od $2^{m-1}n+1$-ve kolone oduzmemo prvu, od $2^{m-1}n+2$-ge kolone oduzmemo drugu,..., od $2^{m-1}n+r$-te kolone oduzmemo r-tu ($r<2^{m-1}n$), razvijajući potom, determinantu po prvih r vrsta, dobijamo

$$R=\begin{vmatrix} -1 & & & -1 & & & 1 \\ -1 & & & & & & \\ & \ddots & & & \ddots & & \\ & & & \mathbf{0} & & & \\ & & & & & & -1 \\ 1 & \cdots & & & & & \\ & \ddots & & & & & \\ & & \mathbf{0} & & & & \\ \mathbf{0} & & & & & & \\ & & 1 & & -1 & & -1 \end{vmatrix} = B_{m,n,r}.$$

U drugom slučaju je

$$R = \begin{vmatrix} 1 & 0 & 0 \ldots 0 & 1 & 0 \ldots\ldots\ldots\ldots\ldots 0 & 0 \\ 0 & 1 & 0 \ldots 0 & 0 & 1 \ldots\ldots\ldots\ldots\ldots 0 & 0 \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ 0 & 0 & 0 \ldots\ldots\ldots\ldots\ldots 1 & 0 & 0 \ldots 0 & 1 \\ 1 & 0 & 0 \ldots\ldots\ldots\ldots\ldots -1 & -1 & 0 \ldots 0 & 0 \\ 0 & 1 & 0 \ldots\ldots\ldots\ldots\ldots 0 & -1 & -1 \ldots 0 & 0 \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ 0 & 0 & 0 \ldots 1 & 0 & 0 \ldots\ldots\ldots\ldots\ldots -1 & -1 \end{vmatrix} \begin{matrix} \\ \\ r \text{ vrsta} \\ \\ \\ \\ 2^{m-1}n \text{ vrsta} \\ \\ \end{matrix}$$

Oduzmimo od $2^{m-1}n+1$-ve kolone prvu, od $2^{m-1}n+2$-ge kolone drugu, ..., od $2^{m-1}n+r$-te kolone r-tu. Kako je $2^{m-1}n<r<2\cdot 2^{m-1}n$,to se element 1 iz prve kolone i $r+1$-ve vrste "preselio" dva puta: prvi put sa znakom minus u $2^{m-1}n+1$-vu kolonu, a zatim sa njom sa znakom plus u $2^{m-1}n+2^{m-1}n+1=2^{m}n+1$-vu kolonu. Razvijajući potom, determinantu po prvih r vrsta, dobijamo determinantu $2^{m}n$-tog reda u kojoj se uočena "jedinica" nalazi u $2^{m}n+1-r$-toj koloni.Znači,

$$R = \begin{vmatrix} -1 & & & & 1 & & & 1 \\ -1 & \ddots & & & & \ddots & & \\ & \ddots & \ddots & & & & \mathbf{0} & \\ & & \ddots & \ddots & & & & \\ & & & \mathbf{0} & & & & 1 \\ & -1 & & & \ddots & & \ddots & \\ & & \ddots & & & \ddots & & \\ & & & \mathbf{0} & & & & \\ \mathbf{0} & & \ddots & & -1 & & -1 & -1 \end{vmatrix} = B_{m,n,r}.$$

Dakle, u oba slučaja dobili smo $R=B_{m,n,r}$, pa iz (2.48) sledi da za neko $r \in S_1$ važi $B_{m,n,r} \equiv 0 \pmod q$. No, onda je $B_{m,n} \equiv 0 \pmod q$, što protivreči uslovu teoreme (2.31).

Preostalo je da (2.46) ne važi. Drugim rečima, kongruencije

$$t^{2^{m-1}} \equiv -1 \pmod q, \quad (t+1)^{2^{m-1}n} \equiv -1 \pmod q \qquad (2.49)$$

imaju zajedničko rešenje.

Pre svega, mora biti $n \geq 5$. Stvarno za $n=1$ (2.49) predstavlja (2.45), pa, kao što smo videli, mora biti $B_{m,1} \not\equiv 0 \pmod q$, što je nemoguće. Takodje, mora biti $m \geq 3$, pošto za $m=2$ (2.49) daje

$$t^2 \equiv -1 \pmod q \Rightarrow (t+1)^2 \equiv 2t \pmod q \Rightarrow$$

$$\Rightarrow -1 \equiv (t+1)^{2n} \equiv (2t)^n \pmod q \Rightarrow 2^{2n} \equiv 1 \pmod q,$$

što protivreči uslovu (2.31).

Iz (2.49) sledi da postoji $r \in S_2$, gde je S_2 odredjen definicijom 2.6, takvo da kongruencije

$$t^{2^{m-1}} \equiv -1 \pmod q, \quad t^r \equiv (t+1)^n \pmod q \tag{2.50}$$

imaju zajedničko rešenje.

Ako je $n>2^{m-1}$, reducirajući kongruencije (2.50) dobijamo

$$t^{2^{m-1}} \equiv -1 \pmod q, \quad \sum_{i=o}^{2^{m-1}-1} a_i t^i \equiv 0 \pmod q, \tag{2.51}$$

gde je za $i \neq r$

$$a_i = \binom{n}{i} - \binom{n}{2^{m-1}+i} + \binom{n}{2^{m-1}2+i} - \dots = \sum_{j=o}^{\infty} \binom{n}{2^{m-1}j+i} (-1)^j, \tag{2.52}$$

a za $i = r$

$$a_r = -1 + \binom{n}{r} - \binom{n}{2^{m-1}+r} + \binom{n}{2^{m-1}2+r} - \dots = -1 + \sum_{j=o}^{\infty} \binom{n}{2^{m-1}j+r} (-1)^j. \tag{2.53}$$

Ako je $n<2^{m-1}$, (2.50) takodje daje (2.51), gde su a_i odredjeni sa (2.52) i (2.53). Naime, zapisavši (2.50) u obliku (2.51) izlazi za $i \neq r$

$$a_i = \binom{n}{i} = \sum_{j=o}^{\infty} (-1)^j \binom{n}{2^{m-1}j+i},$$

a za $i = r$

$$a_r = \binom{n}{r} - 1 = -1 + \sum_{j=o}^{\infty} (-1)^j \binom{n}{2^{m-1}j+r}.$$

Primetimo da su sume u (2.52) i (2.53) konačne, jer je za $2^{m-1}j+i>n$, $\binom{n}{2^{m-1}j+i} = 0$.

Dakle, u svakom slučaju, iz činjenice da kongruencije (2.50) imaju zajedničko rešenje za neko $r \in S_2$, sledi da za neko $r \in S_2$ i kongruencije (2.51) imaju zajedničko rešenje. Znači, za neko $r \in S_2$ rezultanta R' polinoma $t^{2^{m-1}} + 1$ i $\sum_{i=o}^{2^{m-1}-1} a_i t^i$ je deljiva sa q. Imajući na umu definiciju 2.3, lako je uočiti da je

$R'=D_{m,n,r}$. Sledi, za neko $r \in S_2$ važi $D_{m,n,r} \equiv 0 \pmod q$, pa je i $D_{m,n} \equiv 0 \pmod q$, što protivreči uslovu (2.31).

Na taj način pokazali smo da iz pretpostavke da je tvrdjenje teoreme tačno za neki prirodan broj $m-1$ sledi da je tvrdjenje tačno za prirodan broj m, pa kako je tvrdjenje tačno i za $m=1$, to prema principu matematičke indukcije zaključujemo da je tvrdjenje tačno za svaki prirodan broj m. Time je teorema u potpunosti dokazana.

Pre nego zaključimo raspravu o paru kongruencija (2.25) primetimo ovde još nekoliko specijalnih tvrdjenja, koja nisu našla mesto u opštem slučaju kojeg je tretirala teorema 2.2.

Za $m=2$, iz skupa S_1 se mogu isključiti vrednosti $r=n$ i $r=3n$. Naime, za $r=n$ kongruencije (2.47) postaju

$$t^{2n} \equiv -1 \pmod q, \quad t^n \equiv t+1 \pmod q,$$

pa je

$$(t+1)^2 \equiv -1 \pmod q \Rightarrow t^2 \equiv -2(t+1) \pmod q \Rightarrow 2^{4n} \equiv 1 \pmod q,$$

što protivreči uslovu (2.31). Za $r=3n$ (2.47) postaje

$$t^{2n} \equiv -1 \pmod q, \quad t^{3n} \equiv t+1 \pmod q,$$

pa je opet $(t+1)^2 \equiv -1 \pmod q$, što je, videli smo, nemoguće.

Za $m=3$, iz skupa S_1 možemo da isključimo vrednosti $r=2n+1$ i $r=6n+1$. Naime, za $r=2n+1$ kongruencije (2.47) postaju

$$t^{4n} \equiv -1 \pmod q, \quad t^{2n+1} \equiv t+1 \pmod q,$$

pa je

$$-t^2 \equiv (t+1)^2 \pmod q \Rightarrow 2t(t+1) \equiv -1 \pmod q \Rightarrow 2^{4n} \equiv 1 \pmod q,$$

što protivreči uslovu (2.31). Takodje, za $r=6n+1$ kongruencije (2.47) daju

$$t^{4n} \equiv -1 \pmod q, \quad t^{6n+1} \equiv t+1 \pmod q,$$

pa je opet $-t^2 \equiv (t+1)^2 \pmod q$, što je nemoguće.

2.4 Primena na prvi slučaj Fermat-ovog problema

Naš sledeći korak biće da povežemo rezultate teorema 2.1 i 2.2. Drugim rečima, da primenimo teoremu 2.2 na prvi slu-

čaj Fermat-ovog problema.

Teorema 2.3 Neka je $p \in P$, $p \geq 3$. Ako postoji bar jedan par brojeva $m \in N$ i $n=1$, $n \in P$, $n \geq 5$, takvih da je $q=2^m np+1$ prost broj i ako je pri tom

$$A_n \hat{B}_{m,n} C_n D_{m,n} (2^{2^m n}-1)\left[(2^m n)^{2^m n}-1\right] \not\equiv 0 \pmod{q}, \qquad (2.54)$$

tada jednačina

$$x^p + y^p = z^p, \quad x,y,z \in N. \qquad (2.55)$$

nema rešenja relativno prosta sa p.

Dokaz. Za $p=3$ tvrdjenje je tačno. Naime, s jedne strane,za prost broj $q=2\cdot 3+1=7$ je ispunjen uslov (2.54), jer je $2^2 - 1 \not\equiv 0 \pmod 7$. S druge strane, kongruencije $t^2 \equiv 1 \pmod 7$, $(t+1)^2 \equiv 1 \pmod 7$, očigledno nemaju zajedničko rešenje i pri tome je $2^2 \not\equiv 1 \pmod 7$, pa na osnovu teoreme 2.1 za $s=2$ zaključujemo da jednačina (2.55) nema rešenja relativno prosta sa $p=3$.

Neka je sad $p \in P$, $p \geq 5$. Zbog uslova (2.54), na osnovu teoreme 2.2 za $k=m$, sledi da kongruencije

$$t^{2^m n} \equiv 1 \pmod q, \quad (t+1)^{2^m n} \equiv 1 \pmod q,$$

gde je $q=2^m np+1$ prost broj, nemaju zajedničko rešenje. Kako je pri tom

$$(2^m n)^{2^m n} - 1 \not\equiv 0 \pmod q,$$

to na osnovu teoreme 2.1 za $s=2^m n$ sledi da jednačina (2.55) nema rešenja relativno prosta sa p. Time je teorema u potpunosti dokazana.

Ovde sa pravom može da se postavi pitanje, koliko je efikasna teorema 2.3. Drugim rečima, postavlja se pitanje, da li je provera uslova (2.54) dovoljno jednostavna, da bi bila praktično primenljiva. Prisetimo se, veličine $A_{n,r}$, $B_{m,n,r}$ i $C_{n,r}$, pa, dakle i A_n, $B_{m,n}$ i C_n se vrlo lako izračunavaju na osnovu lema 2.3, 2.4 i 2.5, šta više, za njihovo izračunavanje moguće je vrlo efikasno, po potrebi, iskoristiti računar. Isto tako, izračunavanje $2^{2^m n} - 1$ ne predstavlja nikakvu teškoću.

Problemi objektivno nastaju jedino kod izračunavanja veličina $D_{m,n,r}$, odnosno $D_{m,n}$, za $m \geq 5$, $n \geq 5$, jer u tim slučajevima jednakost (2.23) ne obezbedjuje lako izračunavanje. Za

$m=1$, $m=2$, ili za $n=1$, $D_{m,n}=1$; za $m=3$ imamo na raspolaganju jednakost (2.24), dok se za $m=4$ (2.23) može dosta jednostavno da izračuna.

Što se tiče veličina $(2^m n)^{2^m n}-1$, njih u krajnjoj liniji ne moramo da faktorišemo, jer se za konkretno p i q lako proverava da li je $(2^m n)^{2^m n}-1 \equiv 0 \pmod q$.

Uostalom, da potvrdimo ono što smo rekli, mi ćemo teoremu 2.3 odmah da konkretizujemo.

Teorema 2.4 Neka je $p \in P$, $p \geq 3$ i neka je $n=1$, $1 \leq m \leq 6$; $n=5$, $1 \leq m \leq 3$; $n=7$, $n=11$, $1 \leq m \leq 2$; $13 \leq n \leq 23$, $n \in P$, $m=1$. Ako je bar jedan od brojeva $q=2^m np+1$ prost i ako je pri tom

$$(2^m n)^{2^m n}-1 \not\equiv 0 \pmod q, \tag{2.56}$$

tada jednačina (2.55) nema rešenja relativno prosta sa p.

Dokaz. Na osnovu teoreme 2.3 dovoljno je pokazati da je za navedene vrednosti m i n ispunjeno

$$A_n B_{m,n} C_n D_{m,n} (2^{2^m n}-1) \not\equiv 0 \pmod q. \tag{2.57}$$

Izračunajmo* redom potrebne elemente.

1^o $n=1$, $1 \leq m \leq 6$. Ovde je po definiciji $A_1 = C_1 = D_{m,1} = 1$. Takodje, za $m=1$, $m=2$ je $B_{m,1}=1$. Za $m=3$ je $S_1=\{7\}$, i pri tome je

$$B_{3,1,7} = 3^2 = (2+1)^2.$$

Za $m=4$, $S_1=\{3,5,15\}$ i pri tome je

$$B_{4,1,3} = B_{4,1,5} = 17 = 2^4+1,$$

$$B_{4,1,15} = 49 = 7^2 = (2\cdot 3+1)^2.$$

Za $m=5$, $S_1=\{3,5,7,9,19,21,31\}$, pa dobijamo redom

$$B_{5,1,3} = B_{5,1,21} = 97 = 2^5 3+1,$$

$$B_{5,1,5} = 193 = 2^6 3+1,$$

$$B_{5,1,7} = 353 = 2^5 11+1,$$

$$B_{5,1,9} = 257 = 2^8+1,$$

---

* Račun je izveden korišćenjem malog "digitrona" i ceo posao je trajao oko 17 časova.

$$B_{5,1,19} = 449 = 2^6 7 + 1,$$

$$B_{5,1,31} = 2209 = 47^2 = (2 \cdot 23 + 1)^2.$$

Za $m=6$, $S_1 = \{3,5,7,9,11,15,17,19,21,23,25,29,37,51,63\}$. Izlazi

$$B_{6,1,3} = B_{6,1,37} = 7937 = 2^8 31 + 1,$$

$$B_{6,1,5} = 63361 = 2^7 3^2 5 \cdot 11 + 1,$$

$$B_{6,1,7} = 65921 = 2^7 5 \cdot 103 + 1,$$

$$B_{6,1,9} = 21569 = 2^6 337 + 1,$$

$$B_{6,1,11} = 204353 = 2^6 31 \cdot 103 + 1,$$

$$B_{6,1,15} = 123713 = 193 \cdot 641 = (2^6 3 + 1)(2^7 5 + 1),$$

$$B_{6,1,17} = 65537 = 2^{16} + 1,$$

$$B_{6,1,19} = 49601 = 193 \cdot 257 = (2^6 3 + 1)(2^8 + 1),$$

$$B_{6,1,21} = 33409 = 2^7 3^2 29 + 1,$$

$$B_{6,1,23} = 27457 = 2^6 3 \cdot 11 \cdot 13 + 1,$$

$$B_{6,1,25} = 15809 = 2^6 13 \cdot 19 + 1,$$

$$B_{6,1,29} = 48449 = 2^6 757 + 1,$$

$$B_{6,1,51} = 65441 = 31 \cdot 2111 = (2 \cdot 3 \cdot 5 + 1)(2 \cdot 5 \cdot 211 + 1),$$

$$B_{6,1,63} = 4870849 = 2207^2 = (2 \cdot 1103 + 1)^2.$$

Imajući na umu da je za $m \geq 3$

$$B_{m,1} = \prod_{i=3}^{m} \left[\prod_{r \in S_1} B_{i,1,r} \right],$$

to izlazi

$B_{3,1} \not\equiv 0 \pmod q$ za svako $q = 2^3 p + 1$;

$B_{4,1} \not\equiv 0 \pmod q$ za svako $q = 2^4 p + 1$;

$B_{5,1} \equiv 0 \pmod{2^5 p + 1}$ za $p=3$, $p=11$;

$B_{6,1} \equiv 0 \pmod{2^6 p + 1}$ za $p=3$, $p=7$, $p=337$, $p=757$.

Takodje važi

$$2^{2^m} - 1 \not\equiv 0 \pmod{2^m p + 1}, \quad 1 \leq m \leq 6.$$

Stvarno, brojevi $2 + 1$, $2^2 + 1$, $2^{2^2} + 1$, $2^{2^3} + 1$, $2^{2^4} + 1$ su prosti

i nisu oblika $2^m p+1$, $1 \leqslant m \leqslant 6$, a broj $2^{2^5} + 1 = 641 \cdot 6700417 = (2^7 5 + 1)(2^7 52347 + 1)$, takodje nije deljiv ni jednim prostim faktorom oblika $2^m p+1$, $1 \leqslant m \leqslant 6$.

2^0 $n=5$, $1 \leqslant m \leqslant 3$. Ovde je po definiciji $C_5 = 1$, $D_{1,5} = D_{2,5} = 1$, $B_{1,5} = 1$. Takodje je

$$A_5 = A_{5,2} = 11 = 2 \cdot 5 + 1 \not\equiv 0 \pmod{q}$$

za svako $q = 2^m 5p+1$, $1 \leqslant m \leqslant 3$. Za $m=2$ je $S_1 = \{3, 13, 19\}$, pa izlazi

$$B_{2,5,3} = 25 = 5^2 = (2^2 + 1)^2,$$

$$B_{2,5,13} = 61 = 2^2 3 \cdot 5 + 1,$$

$$B_{2,5,19} = 125 = 5^3 = (2^2 + 1)^3.$$

Za $m=3$ je $S_1 = \{3, 5, 7, 9, 13, 15, 17, 25, 29, 35, 39\}$, pa dobijamo

$$B_{3,5,3} = B_{3,5,25} = 281 = 2^3 5 \cdot 7 + 1,$$

$$B_{3,5,5} = B_{3,5,13} = 697 = 17 \cdot 41 = (2^4 + 1)(2^3 5 + 1),$$

$$B_{3,5,7} = 2169 = 3^2 241 = (2 + 1)^2 (2^4 5 \cdot 3 + 1),$$

$$B_{3,5,9} = 1681 = 41^2 = (2^3 5 + 1)^2,$$

$$B_{3,5,15} = 369 = 3^2 41 = (2 + 1)^2 (2^3 5 + 1),$$

$$B_{3,5,17} = 881 = 2^4 5 \cdot 11 + 1,$$

$$B_{3,5,29} = 1377 = 3^4 17 = (2 + 1)^4 (2^4 + 1),$$

$$B_{3,5,35} = 641 = 2^7 5 + 1,$$

$$B_{3,5,39} = 15129 = 3^2 41^2 = (2 + 1)^2 (2^3 5 + 1)^2.$$

Dalje neposredno dobijamo

$$B_{2,5} \equiv 0 \pmod{2^2 5p+1} \text{ za } p=3;$$

$$B_{3,5} \equiv 0 \pmod{2^3 5p+1} \text{ za } p=7.$$

Prema formulama (2.52) i (2.53) za $m=3$, $n=5$ izlazi za $r=1$

$$a_0 = -4, \ a_1 = 3, \ a_2 = 10, \ a_3 = 10,$$

a za $r=3$

$$a_0 = -4, \ a_1 = 4, \ a_2 = 10, \ a_3 = 9,$$

pa na osnovu (2.24) dobijamo

$$D_{3,5,1} = 697 = 17 \cdot 41 = (2^4 + 1)(2^3 5 + 1),$$

$$D_{3,5,3} = 369 = 3^2 41 = (2 + 1)^2 (2^3 5 + 1).$$

Očigledno, $D_{3,5} \not\equiv 0 \pmod q$, za svako $q=2^3 5p+1$. Takodje je

$$2^{10}-1 = 3\cdot 11\cdot 31 = (2+1)(2\cdot 5+1)(2\cdot 5\cdot 3+1) \equiv 0 \pmod{2\cdot 5p+1} \text{ za } p=3;$$

$$2^{20}-1 = 3\cdot 5^2 11\cdot 31\cdot 41 = (2+1)(2^2+1)^2(2\cdot 5+1)(2\cdot 5\cdot 3+1)(2^3 5+1) \not\equiv 0 \pmod q \text{ za svako } q=2^2 5p+1;$$

$$2^{40}-1 = 3\cdot 5^2 11\cdot 17\cdot 31\cdot 41\cdot 61681 = (2+1)(2^2+1)^2(2\cdot 5+1)(2^4+1)(2\cdot 5\cdot 3+1)(2^3 5+1)(2^4 5\cdot 3\cdot 257+1) \not\equiv 0 \pmod q \text{ za svako } q=2^3 5p+1.$$

3° $n=7$, $1\leqslant m\leqslant 2$. Ovde je po definiciji $D_{1,7}= D_{2,7}= B_{1,7}= 1$. Kako je

$$A_{7,2}= 29 = 2^2 7+1,$$

$$A_{7,3}= 2^3,$$

to je

$$A_7 \not\equiv 0 \pmod q \text{ za svako } q=2^m 7p+1,\ 1\leqslant m\leqslant 2.$$

Dalje je $S=\{3\}$, pa izlazi

$$C_7= C_{7,3}= 2^3 \not\equiv 0 \pmod q \text{ za svako } q=2^m 7p+1,\ 1\leqslant m\leqslant 2.$$

Za $m=2$ je $S_1= \{3,5,9,11,27\}$, pa dobijamo

$$B_{2,7,3}= 40 = 2^3 5 = 2^3(2^2+1),$$

$$B_{2,7,5}= 232 = 2^3 29 = 2^3(2^2 7+1),$$

$$B_{2,7,9}= 197 = (2^2 7\cdot 7+1),$$

$$B_{2,7,11}= 145 = 5\cdot 29 = (2^2+1)(2^2 7+1),$$

$$B_{2,7,27}= 845 = 5\cdot 13^2 = (2^2+1)(2^2 3+1)^2.$$

Izlazi

$$B_{2,7} \equiv 0 \pmod{2^2 7p+1} \text{ za } p=7.$$

Takodje je

$$2^{14}-1 = 3\cdot 43\cdot 127 = (2+1)(2\cdot 7\cdot 3+1)(2\cdot 7\cdot 3^2+1) \equiv 0 \pmod{2\cdot 7p+1} \text{ za } p=3;$$

$$2^{28}-1 = 3\cdot 5\cdot 29\cdot 43\cdot 113\cdot 127 = (2+1)(2^2+1)(2^2 7+1)(2\cdot 7\cdot 3+1)(2^4 7+1)(2\cdot 7\cdot 3^2+1) \not\equiv 0 \pmod q \text{ za svako } q=2^2 7p+1.$$

4° $n=11$, $1\leqslant m\leqslant 2$. Ovde je po definiciji $D_{1,11}= D_{2,11}= B_{1,11}= 1$. Kako je

$$A_{11,2} = 199 = 2\cdot 11\cdot 3^2 + 1,$$

$$A_{11,3} = A_{11,4} = 23 = 2\cdot 11 + 1,$$

$$A_{11,5} = 67 = 2\cdot 11\cdot 3 + 1,$$

to je

$$A_{11} \equiv 0 \pmod{2^m 11p+1},\ 1\leqslant m\leqslant 2,\ \text{za } p=3.$$

Dalje je $S = \{3\}$, pa izlazi

$$C_{11} = C_{11,3} = 23 = 2\cdot 11 + 1 \not\equiv 0 \pmod{q}$$

za svako $q=2^m 11p+1,\ 1\leqslant m\leqslant 2$.

Za $m=2$ je $S_1 = \{3,5,7,13,25,27,29,35,43\}$, pa dobijamo

$$B_{2,11,3} = B_{2,11,27} = 445 = 5\cdot 89 = (2^2+1)(2^3 11 + 1),$$

$$B_{2,11,5} = 2333 = 2^2 11\cdot 53 + 1,$$

$$B_{2,11,7} = 1765 = 5\cdot 353 = (2^2+1)(2^5 11 + 1),$$

$$B_{2,11,13} = 3257 = 2^3 11\cdot 37 + 1,$$

$$B_{2,11,25} = 4357 = 2^2 11^2 3^2 + 1,$$

$$B_{2,11,29} = 1013 = 2^2 11\cdot 23 + 1,$$

$$B_{2,11,35} = 3085 = 5\cdot 617 = (2^2+1)(2^3 11\cdot 7 + 1),$$

$$B_{2,11,43} = 39605 = 5\cdot 89^2 = (2^2+1)(2^3 11 + 1)^2.$$

Izlazi

$$B_{2,11} \equiv 0 \pmod{2^2 11p+1} \text{ za } p=23,\ p=53.$$

Takodje je

$$2^{22} - 1 = 3\cdot 23\cdot 89\cdot 683 = (2+1)(2\cdot 11+1)(2^3 11.+$$

$$+ 1)(2\cdot 11\cdot 31 + 1) \equiv 0 \pmod{2\cdot 11p+1} \text{ za } p=31;$$

$$2^{44} - 1 = 3\cdot 5\cdot 23\cdot 89\cdot 397\cdot 683\cdot 2113 = (2+1)(2^2+1)(2\cdot 11+$$

$$+ 1)(2^3 11 + 1)(2^2 11\cdot 3^2 + +)(2\cdot 11\cdot 31 + 1)(2^6 11\cdot 3 + 1) \not\equiv 0$$

$(\text{mod } q)$ za svako $q=2^2 11p+1$.

5° $m=1,\ 13\leqslant n\leqslant 23,\ n\in P$. Ovde je po definiciji $B_{1,n} = D_{1,n} = 1$. Za $n=13$ je $S = \{3,4\}$, pa dobijamo

$$A_{13,2} = 521 = 2^3 13\cdot 5 + 1,$$

$$A_{13,3} = 27 = 3^3 = (2+1)^3,$$

$$A_{13,4} = 79 = 2\cdot 13\cdot 3 + 1,$$

$$A_{13,5} = 53 = 2^2 13 + 1,$$

$$A_{13,6} = 131 = 2 \cdot 13 \cdot 5 + 1,$$

$$C_{13,3} = 53 = 2^2 13 + 1,$$

$$C_{I3,4} = 27 = 3^3 = (2 + 1)^3.$$

Izlazi

$$A_{13} C_{13} \equiv 0 \pmod{2 \cdot 13p+1} \text{ za } p=3,\ p=5.$$

Za $n=17$ je $S = \{3,4\}$, pa dobijamo

$$A_{17,2} = 3571 = 2 \cdot 17 \cdot 3 \cdot 5 \cdot 7 + 1,$$

$$A_{17,3} = A_{17,4} = 137 = 2^3 17 + 1,$$

$$A_{17,5} = 307 = 2 \cdot 17 \cdot 3^2 + 1,$$

$$A_{17,6} = 103 = 2 \cdot 17 \cdot 3 + 1,$$

$$A_{17,7} = 409 = 2^3 17 \cdot 3 + 1,$$

$$A_{17,8} = 613 = 2^2 17 \cdot 3^2 + 1,$$

$$C_{17,3} = 239 = 2 \cdot 17 \cdot 7 + 1,$$

$$C_{17,4} = 103 = 2 \cdot 17 \cdot 3 + 1.$$

Izlazi

$$A_{17} C_{17} \equiv 0 \pmod{2 \cdot 17p+1} \text{ za } p=3,\ p=7.$$

Za $n=19$ je $S = \{3,4,8\}$, pa dobijamo

$$A_{19,2} = 9349 = 2^2 19 \cdot 3 \cdot 41 + 1,$$

$$A_{19,3} = A_{19,6} = 229 = 2^2 19 \cdot 3 + 1,$$

$$A_{19,4} = 761 = 2^3 19 \cdot 5 + 1,$$

$$A_{19,5} = 647 = 2 \cdot 19 \cdot 17 + 1,$$

$$A_{19,7} = C_{19,4} = 191 = 2 \cdot 19 \cdot 5 + 1,$$

$$A_{19,8} = 419 = 2 \cdot 19 \cdot 11 + 1,$$

$$A_{19,9} = 1483 = 2 \cdot 19 \cdot 3 \cdot 13 + 1,$$

$$C_{19,3} = 457 = 2^3 19 \cdot 3 + 1,$$

$$C_{19,8} = 343 = 7^3 = (2 \cdot 3 + 1)^3.$$

Izlazi

$$A_{19} C_{19} \equiv 0 \pmod{2 \cdot 19p+1} \text{ za } p=5,\ p=11,\ p=17.$$

Za $n=23$ je $S = \{3,4,5\}$, pa dobijamo

$$A_{23,2} = 64079 = 139\cdot 461 = (2\cdot 23\cdot 3 + 1)(2^2 23\cdot 5 + 1),$$

$$A_{23,3} = A_{23,7} = 599 = 2\cdot 23\cdot 13 + 1,$$

$$A_{23,4} = 2347 = 2\cdot 23\cdot 3\cdot 17 + 1,$$

$$A_{23,5} = A_{23,6} = C_{23,3} = 2209 = 47^2 = (2\cdot 23 + 1)^2,$$

$$A_{23,8} = C_{23,5} = 691 = 2\cdot 23\cdot 3\cdot 5 + 1,$$

$$A_{23,9} = 1151 = 2\cdot 23\cdot 5^2 + 1,$$

$$A_{23,10} = 3313 = 2^4 23\cdot 3^2 + 1,$$

$$A_{23,11} = 6533 = 47\cdot 139 = (2\cdot 23 + 1)(2\cdot 23\cdot 3 + 1),$$

$$C_{23,4} = 829 = 2^2 23\cdot 3^2 + 1.$$

Izlazi

$$A_{23}C_{23} \equiv 0 \pmod{2\cdot 23p+1} \text{ za } p=3,\ p=13.$$

Dalje dobijamo

$$2^{26} - 1 = 3\cdot 2731\cdot 8191 = (2+1)(2\cdot 13\cdot 3\cdot 5\cdot 7 + 1)(2\cdot 13\cdot 3^2 5\cdot 7 + 1) \not\equiv 0 \pmod{q}$$ za svako $q=2\cdot 13p+1$;

$$2^{34} - 1 = 3\cdot 43691\cdot 131071 = (2+1)(2\cdot 17\cdot 5\cdot 257 + 1)(2\cdot 17\cdot 3\cdot 5\cdot 257 + 1) \not\equiv 0 \pmod{q}$$ za svako $q=2\cdot 17p+1$;

$$2^{38} - 1 = 3\cdot 174763\cdot 524287 = (2+1)(2\cdot 19\cdot 3^2 7\cdot 73 + 1)(2\cdot 19\cdot 3^3 7\cdot 73 + 1) \not\equiv 0 \pmod{q}$$ za svako $q=2\cdot 19p+1$;

$$2^{46} - 1 = 3\cdot 47\cdot 178481\cdot 2796203 = (2+1)(2\cdot 23 + 1)(2^4 23\cdot 5\cdot 97 + 1)(2\cdot 23\cdot 89\cdot 683 + 1) \not\equiv 0 \pmod{q}$$ za svako $q=2\cdot 23p+1$.

Preostalo je još da rezimiramo za koje vrednosti p, m i n nije zadovoljen uslov (2.57). Preglednosti radi, prikažimo to tabelarno.

p	$m,\ n$	p	$m,\ n$
3	5, 1; 6, 1; 1, 5; 2, 5; 1, 7; 1, 11; 1, 13; 1, 17; 1, 23	17	1, 19
		23	2, 11
5	1, 13; 1, 19	31	1, 11
7	6, 1; 3, 5; 2, 7; 1, 17	53	2, 11
11	5, 1; 1, 19	337	6, 1
13	1, 23	757	6, 1

Znači, za navedene vrednosti p, m, n ne možemo iskoristiti činjenicu da je $2^m np+1$ prost broj. Medjutim, za sve navedene vrednosti p, postoje druge vrednosti m, n takve da je $2^m np+1$ prost broj. Imamo redom

$$p=3,\ m=n=1;\ p=5,\ m=n=1;\ p=7,\ m=2,\ n=1;\ p=11,\ m=n=1;$$
$$p=13,\ m=2,\ n=1;\ p=17,\ m=3,\ n=1;\ p=23,\ m=n=1;\ p=31,$$
$$m=1,\ n=5;\ p=53,\ m=n=1;\ p=337,\ m=1,\ n=5;\ p=757,\ m=4,n=1.$$

Time je teorema u potpunosti dokazana.

Primetimo ovde, da bi uslov (2.56), za veći broj vrednosti m, n navedenih u teoremi 2.4, mogao da se izbegne izračunavanjem veličine $(2^m n)^{2^m n} - 1$ i rešavanjem kongruencije (2.56). Stvarno, imajući na umu lemu 1.5, prema kojoj su svi prosti faktori broja

$$[(2^m n)^{2^m n} - 1][(2^m n)^{2^m} - 1]^{-1}, \quad n \geq 5, \quad n \in P,$$

oblika $2\lambda n+1$, dobijamo redom

$$10^{10} - 1 = 3^2 11 \cdot 9091 \cdot 11111 = (2+1)^2(2\cdot 5 + 1)(2\cdot 5\cdot 3^2 101 + 1)(2\cdot 5\cdot 11\cdot 101 + 1),$$

$$20^{20} - 1 = 3\cdot 7\cdot 11\cdot 19\cdot 41\cdot 61\cdot 251\cdot 401\cdot 2801\cdot 152381\cdot 222361 =$$
$$= (2+1)(2\cdot 3+1)(2\cdot 5+1)(2\cdot 3^2+1)(2^3 5+1)(2^2 5\cdot 3+1)(2\cdot 5^3+1)(2^4 5^2+1)(2^4 5^2 7+1)(2^2 5\cdot 19\cdot 401+1)(2^3 5\cdot 3\cdot 17\cdot 109+1),$$

$$28^{28} - 1 = 5\cdot 29\cdot 157\cdot 281\cdot 13007\cdot 35771\cdot 749729\cdot 1100860153 =$$
$$= (2^2+1)(2^2 7+1)(2^2 3\cdot 13+1)(2^3 7\cdot 5+1)(2\cdot 7\cdot 929+1)(2\cdot 7^2 5\cdot 73+1)(2^5 7\cdot 3347+1)(2^3 7\cdot 3\cdot 19\cdot 353\cdot 977+1),$$

$$22^{22} - 1 = 3\cdot 7\cdot 23\cdot 89\cdot 285451051007\cdot 27824681019587 =$$
$$= (2+1)(2\cdot 3+1)(2\cdot 11+1)(2^3 11+1)(2\cdot 11\cdot 911\cdot 14242643+1)(2\cdot 11\cdot 23\cdot 54989488181+1).$$

Rešavajući kongruenciju (2.56) za odgovarajuće vrednosti m, n, dobijamo da rešenje postoji jedino u slučaju kada je $m=2$, $n=5$, $p=3$, što je, kao što smo videli u dokazu teoreme 2.4, bez značaja.

Razmotrimo još uslov (2.56) za $n=1$, $1\leqslant m\leqslant 6$. Pokažimo da je

$$2^{m2^m} - 1 \not\equiv 0 \pmod{q},\ q=2^m p+1,\ 1\leqslant m\leqslant 6. \qquad (2.58)$$

Pre svega, imajmo na umu da svi prosti faktori broja

$$F_k = 2^{2^k} + 1$$

su oblika $2^{k+2}\lambda+1$ ([7], Vol.I, 376). Kako su F_i, $0\leqslant i\leqslant 4$, prosti brojevi koji očigledno nisu oblika $2^m p+1$, to na osnovu navedene osobine brojeva F_k, zaključujemo da je

$$F_k \not\equiv 0 \pmod{2^m p+1},\ 1\leqslant m\leqslant 6,\ 0\leqslant k\leqslant 6.$$

No, onda je

$$a_k = 2^{2^k} - 1 = \prod_{i=0}^{k-1} F_i \not\equiv 0 \pmod{2^m p+1},\ 1\leqslant m\leqslant 6,\ 1\leqslant k\leqslant 7. \qquad (2.59)$$

Kako je

$$\begin{aligned}
2^2 - 1 &= a_1,\\
2^{2\cdot 2^2} - 1 &= a_3,\\
2^{3\cdot 2^3} - 1 &= (2^8 - 1)(2^{16} + 2^8 + 1) = a_3 a,\\
2^{4\cdot 2^4} - 1 &= a_6,\\
2^{5\cdot 2^5} - 1 &= (2^{32} - 1)(2^{128} + 2^{96} + 2^{64} + 2^{32} + 1) = a_5 b,\\
2^{6\cdot 2^6} - 1 &= (2^{128} - 1)(2^{256} + 2^{128} + 1) = a_7 c,
\end{aligned}$$

to na osnovu (2.59) izlazi da je uslov (2.58) zadovoljen za $m=1,2,4$. Takodje iz

$$a \equiv 0 \pmod{8p+1},\ b \equiv 0 \pmod{32p+1},\ c \equiv 0 \pmod{64p+1},$$

sledi, na osnovu leme 1.5, kao jedino eventualno rešenje $p=3$, $p=5$, $p=3$, respektivno, što je, u krajnjoj liniji, bez značaja. No, to znači da je uslov (2.58) zadovoljen za svako m, $1\leqslant m\leqslant 6$.

Sa ovim razmatranjem uslova (2.56), imajući na umu teoremu 2.4, dokazana je sledeća teorema.

Teorema 2.5 Neka je $p\in P$, $p\geqslant 3$. Ako je bar jedan od brojeva $sp+1$, $s=2,4,8,10,14,16,20,22,28,32,64$ prost, tada jednačina (2.55) nema rešenja relativno prosta sa p.

Sada je jasno, da se primenom savršenijih računskih

sredstava, teorema 2.3 može konkretizovati u mnogo širem obliku, nego što smo to mi (primera radi) uradili iskazujući teoreme 2.4 i 2.5. No, i pored toga, na osnovu teorema 2.4 i 2.5 moguće je pokazati da u prvom slučaju Fermat-ovog problema nema rešenja za dosta veliki broj prostih brojeva p. Tako, na primer, od 167 prostih neparnih brojeva manjih od *1000*, samo dva, *383* i *751*, ne padaju pod udar teorema 2.4 i 2.5.

U narednoj tabeli navedeni su svi prosti brojevi $p \geq 3$, manji od *1000* i uz njih najmanja vrednost $2^m n$ takva, da je $2^m np+1$ prost broj.

p	$2^m n$	p	$2^m n$	p	$2^m n$	p	$2^m n$	p	$2^m n$	p	$2^m n$	p	$2^m n$
3	2	101	8	229	22	373	4	521	32	673	4	839	32
5	2	103	10	233	2	379	28	523	10	677	8	853	4
7	4	107	8	239	2	383	/	541	28	683	2	857	8
11	2	109	10	241	10	389	38	547	4	691	10	859	22
13	4	113	2	251	2	397	16	557	8	701	32	863	32
17	8	127	4	257	38	401	8	563	14	709	4	877	16
19	10	131	2	263	20	409	4	569	44	719	2	881	26
23	2	137	8	269	8	419	2	571	10	727	4	883	4
29	2	139	4	271	10	421	10	577	4	733	10	887	26
31	10	149	8	277	4	431	2	587	14	739	4	907	34
37	4	151	10	281	2	433	4	593	2	743	2	911	2
41	2	157	10	283	34	439	10	599	14	751	/	919	4
43	4	163	4	293	2	443	2	601	10	757	16	929	8
47	14	167	14	307	4	449	8	607	40	761	2	937	10
53	2	173	2	311	20	457	46	613	10	769	10	941	8
59	14	179	2	313	16	461	20	617	8	773	20	947	8
61	16	181	10	317	26	463	64	619	4	787	28	953	2
67	4	191	2	331	16	467	20	631	10	797	14	967	16
71	8	193	4	337	10	479	8	641	20	809	2	971	20
73	4	197	38	347	8	487	4	643	16	811	10	977	8
79	4	199	4	349	10	491	2	647	14	821	8	983	14
83	2	211	10	353	14	499	4	653	2	823	10	991	22
89	2	223	34	359	2	503	14	659	2	827	14	997	4
97	4	227	26	367	10	509	2	661	22	829	10		

III G L A V A

3.1 Niz $x_{n,k}$

Ovde će, kao što je istaknuto u Uvodu, biti reči o jednom nizu brojeva, čije će nam osobine omogućiti da izvedemo odgovarajuće rezultate vezane za prvi slučaj Fermat-ovog problema.

Definicija 3.1 Pod $x_{n,k}$, $n,k \in N$, podrazumevaćemo niz

$$x_{n,k} = n^k - \binom{n}{1}(n-1)^k + \binom{n}{2}(n-2)^k - \binom{n}{3}(n-3)^k + \ldots + (-1)^{n-1}\binom{n}{n-1}1^k. \qquad (3.1)$$

Iz (3.1) je očigledno $x_{1,k} = 1$ za svako k. Dokažimo odmah jednu interesantnu osobinu niza $x_{n,k}$.

Lema 3.1 Za svako $k \in N$ i svako $n>k$, $x_{n,k} = 0$.

Dokaz. Lemu ćemo dokazati metodom matematičke indukcije po k. Za $k=1$ i svako $n>1$ imamo

$$x_{n,1} = n - \binom{n}{1}(n-1) + \binom{n}{2}(n-2) - \ldots + (-1)^{n-1}\binom{n}{n-1}1 =$$

$$= n\left[1 - \binom{n-1}{1} + \binom{n-1}{2} - \ldots + (-1)^{n-1}\binom{n-1}{n-1}\right] = n(1-1)^{n-1} = 0.$$

Pretpostavimo da je tvrdjenje tačno za neko $k-1$, $k\geq 2$, tj. neka za svako $n>k-1$ važi $x_{n,k-1} = 0$. Dokažimo da je tvrdjenje tačno za prirodan broj k. Imamo

$$x_{n,k} = n^k - \binom{n}{1}(n-1)^k + \binom{n}{2}(n-2)^k - \ldots + (-1)^{n-1}\binom{n}{n-1}1^k =$$

$$= n\left[n^{k-1} - \binom{n-1}{1}(n-1)^{k-1} + \binom{n-1}{2}(n-2)^{k-1} - \ldots + (-1)^{n-1}\binom{n-1}{n-1}1^{k-1}\right] =$$

$$= n\Big[n^{k-1} - \left[\binom{n}{1} - \binom{n-1}{0}\right](n-1)^{k-1} + \left[\binom{n}{2} - \binom{n-1}{1}\right](n-2)^{k-1} - \ldots +$$

$$+ (-1)^{n-1}\left[\binom{n}{n-1} - \binom{n-1}{n-2}\right]1^{k-1}\Big] = n\Big[\left[n^{k-1} - \binom{n}{1}(n-1)^{k-1} + \binom{n}{2}(n-2)^{k-1} - \right.$$

$$\left. - \ldots + (-1)^{n-1}\binom{n}{n-1}1^{k-1}\right] + \left[(n-1)^{k-1} - \binom{n-1}{1}(n-2)^{k-1} + \ldots + \right.$$

$$\left. + (-1)^{n-2}\binom{n-1}{n-2}1^{k-1}\right]\Big] = n(x_{n,k-1} + x_{n-1,k-1}).$$

Za $n>k$ je $n>k-1$ i $n-1>k-1$, pa je po induktivnoj pretpostavci $x_{n,k-1}= x_{n-1,k-1} = 0$. Sledi, za svako $n>k$ je $x_{n,k}= 0$.

Time je dokazano da iz pretpostavke da je tvrdjenje tačno za neko $k-1$ sledi da je tvrdjenje tačno i za prirodan broj k, pa kako je tvrdjenje važilo i za $k=1$, to prema principu matematičke indukcije sledi da je tvrdjenje tačno za svako $k \in N$.

Lema 3.1 pokazuje da za svako $k \in N$ ima smisla posmatrati samo one $x_{n,k}$ za koje je $1 \leqslant n \leqslant k$, pošto su svi ostali nule. No, niz $x_{n,k}$ krije za nas još neka iznenadjenja. Dokažimo sledeću lemu.

Lema 3.2 Za svako $k \in N$ važi $x_{k,k}= k!$.

Dokaz. U dokazu leme 3.1 pokazano je da niz $x_{n,k}$ zadovoljava rekurentnu formulu

$$x_{n,k}= n(x_{n,k-1}+ x_{n-1,k-1}), \quad n \geqslant 2, \quad k \geqslant 2. \qquad (3.2)$$

Dokažimo lemu matematičkom indukcijom. Za $k=1$, jednakost je tačna, jer je $x_{1,1}= 1 = 1!$. Pretpostavimo da je jednakost tačna za neko $k-1$, $k \geqslant 2$, tj. neka je $x_{k-1,k-1}= (k-1)!$. Iz (3.2), na osnovu leme 3.1, neposredno dobijamo

$$x_{k,k}= k(x_{k,k-1}+ x_{k-1,k-1}) = kx_{k-1,k-1}= k(k-1)! = k!.$$

Dakle, iz pretpostavke da je jednakost tačna za $k-1$, sledi da je jednakost tačna za k, pa kako je jednakost tačna i za $k=1$, to prema principu matematičke indukcije zaključujemo da je jednakost tačna za svako $k \in N$. Time je lema u potpunosti dokazana.

Dakle, dobili smo jednu interesantnu formulu za $k!$. Prema lemi 3.2 važi jednakost

$$k! = k^k - \binom{k}{1}(k-1)^k + \binom{k}{2}(k-2)^k - \ldots + (-1)^{k-1}\binom{k}{k-1}1^k =$$

$$= \sum_{m=1}^{k} (-1)^{k-m}\binom{k}{m}m^k, \quad k \in N. \qquad (3.3)$$

Jednakost (3.3) pruža interesantne mogućnosti za ispitivanje funkcije $n!$. Na primer, poznata Wilson-ova teorema da je

$$(p-1)! \equiv -1 \pmod{p}, \quad p \in P,$$

je na osnovu (3.3) direktna posledica Fermat-ove teoreme da je

$$a^{p-1} \equiv 1 \pmod{p}, \quad (a,p) = 1, \quad p \in P.$$

Naime, iz (3.3) sledi za $k=p-1$, $p \in P$,

$$(p-1)! = (p-1)^{p-1} - \binom{p-1}{1}(p-2)^{p-1} + \binom{p-1}{2}(p-3)^{p-1} - \ldots + (-1)^{p-2}\binom{p-1}{p-2}1^{p-1} \equiv$$

$$\equiv 1 - \binom{p-1}{1} + \binom{p-1}{2} - \ldots + (-1)^{p-2}\binom{p-1}{p-2} = (1-1)^{p-1} - 1 = -1 \pmod{p}.$$

Niz $x_{n,k}$ pored navedenih osobina, ima još neke, same za sebe, interesantne osobine. Mi ćemo kasnije doći u priliku da dokažemo da za niz $x_{n,k}$ važe, na primer, sledeća tvrdjenja:

1° Neka je $1 \leqslant j \leqslant k-n$ i neka je N_j odredjeno sa

$$N_j = \sum \left[\prod_{l=1}^{s} \alpha_l! \left[(m_l + 1)! \right]^{\alpha_l} \right]^{-1},$$

gde se sumiranje vrši po svim slučajevima kada je $s \geqslant 1$, $\alpha_1 + \alpha_2 + \ldots + \alpha_s = j$, $1 \leqslant \alpha_1 \leqslant \alpha_2 \leqslant \ldots \leqslant \alpha_s$, $m_1\alpha_1 + m_2\alpha_2 + \ldots + m_s\alpha_s = k-n$, $m_i \neq m_l$, $\alpha_i = \alpha_l \Rightarrow m_i < m_l$. Tada je

$$x_{n,k} = k! \sum_{j=1}^{k-n} \binom{n}{j} j! N_j, \quad n \leqslant k-1. \tag{3.4}$$

Specijalno, za $n=k-1$, iz (3.4) sledi

$$x_{k-1,k} = k!\binom{k-1}{1}1!N_1 = k!\binom{k-1}{1}1!\,\frac{1}{1!2!} = \frac{k-1}{2}\,k!.$$

Slično bi se iz (3.4) dobile jednakosti za $n=1,2,\ldots k-2$.

2° Neka je

$$D_k(x) = \sum_{n=1}^{k} (-1)^{k-n} x_{n,k} x^{k-n}.$$

Tada je $D_k(2) = 0$ ako i samo ako je k parno.

3° Važi jednakost

$$D_k(1) = \sum_{n=1}^{k} (-1)^{k-n} x_{n,k} = 1,$$

za svako $k \in N$.

3.2 Funkcija $!n$

Neka nam ovde bude dozvoljeno da "otvorimo zagradu" da bi , privremeno napustivši naš osnovni zadatak, razmatranje Fer-

mat-ovog problema, primenili lemu 3.2 na probleme vezane za $!n$.

Dj. Kurepa je u [25] definisao

$$!n = 0! + 1! + 2! + \ldots + (n-1)!, \quad n \in N \tag{3.5}$$

i izmedju ostalog, postavio hipotezu da je

$$(!n, n!) = 2, \text{ za svako } n \in N, \ n \geqslant 2. \tag{3.6}$$

Takodje, u [25] je dato više hipoteza ekvivalentnih hipotezi (3.6), a izmedju ostalih i ova

$$!p \not\equiv 0 \pmod{p}, \text{ za svako } p \in P, \ p \geqslant 3. \tag{3.7}$$

Jednakost (3.3) nam pruža šansu da, pre svega, $!n$ dobijemo u bitno drugačijem obliku od (3.5), a samim tim, da damo novu hipotezu ekvivalentnu sa (3.7), odnosno (3.6).

Teorema 3.1 Neka je

$$A_{n,k} = \binom{k}{0} - \binom{k+1}{1}k + \binom{k+2}{2}k^2 - \binom{k+3}{3}k^3 + \ldots + (-1)^{n-k-1}\binom{n-1}{n-k-1}k^{n-k-1}.$$

Tada je

$$!n = 1 + \sum_{k=1}^{n-1} k^k A_{n,k} = 1 + \sum_{k=1}^{n-1}\sum_{i=0}^{n-k-1} \binom{k+i}{i} k^{i+k}, \quad n \geqslant 2. \tag{3.8}$$

Dokaz. Dokaz izlazi neposrednom primenom jednakosti (3.3). Imamo

$$!n = 1 + 1! + 2! + \ldots + (n-1)! = 1 + \sum_{k=1}^{n-1} x_{k,k} =$$

$$= 1 + 1^1 + [2^2 - \binom{2}{1}1^2] + [3^3 - \binom{3}{1}2^3 + \binom{3}{2}1^3] + \ldots +$$

$$+ [(n-1)^{n-1} - \binom{n-1}{1}(n-2)^{n-1} + \ldots + (-1)^{n-2}\binom{n-1}{n-2}1^{n-1}] =$$

$$= 1 + [1 - \binom{2}{1}1^1 + \binom{3}{2}1^2 - \ldots + (-1)^{n-2}\binom{n-1}{n-2}1^{n-2}]1^1 +$$

$$+ [1 - \binom{3}{1}2^1 + \binom{4}{2}2^2 - \ldots + (-1)^{n-3}\binom{n-1}{n-3}2^{n-3}]2^2 + \ldots +$$

$$+ [1 - \binom{n-1}{1}(n-2)^1](n-2)^{n-2} + (n-1)^{n-1} = 1 + \sum_{k=1}^{n-1} k^k A_{n,k},$$

što je i trebalo dokazati.

Jednakost (3.8), videćemo, moći će da se iskoristi za ispitivanje kongruencije $!p \equiv 0 \pmod{p}$, $p \in P$. Dokažimo stoga, sledeću teoremu.

Teorema 3.2 Neka je $p \in P$, $p \geqslant 3$, i neka je

$$S_p = 1 + 2^{p-2}1^1 + 3^{p-3}2^2 + \ldots + \left(\frac{p-1}{2}\right)^{\frac{p+1}{2}}\left(\frac{p-3}{2}\right)^{\frac{p-3}{2}}.$$

Tada je

$$!p \equiv 2S_p + (-1)^{\frac{p-1}{2}} \pmod p. \tag{3.9}$$

Dokaz. Za $p \in P$, $p \geq 3$, $k < p-1$, očigledno važi

$$\binom{k+m}{m} = \frac{1}{m!}(k+m)(k+m-1)\ldots(k+1) \equiv$$

$$\equiv \frac{(-1)^m}{m!}(p-k-m)(p-k-m+1)\ldots(p-k-1) = (-1)^m\binom{p-k-1}{m} \pmod p.$$

No, onda je

$$A_{p,k} = \binom{k}{o} - \binom{k+1}{1}k + \binom{k+2}{2}k^2 - \ldots + (-1)^{p-k-1}\binom{p-1}{p-k-1}k^{p-k-1} \equiv$$

$$\equiv \binom{p-k-1}{o} + \binom{p-k-1}{1}k + \binom{p-k-1}{2}k^2 + \ldots + \binom{p-k-1}{p-k-1}k^{p-k-1} =$$

$$= (1+k)^{p-k-1} \pmod p, \quad k < p-1.$$

Za $k=p-1$, očigledno je $A_{p,p-1} = 1$.

Na osnovu jednakosti (3.8), sledi

$$!p = 1 + \sum_{k=1}^{n-1} k^k A_{p,k} \equiv 1 + (p-1)^{p-1} + \sum_{k=1}^{p-2}(k+1)^{p-k-1}k^k \equiv$$

$$\equiv 2 + 2^{p-2}1^1 + 3^{p-3}2^2 + \ldots + \left(\frac{p-1}{2}\right)^{\frac{p+1}{2}}\left(\frac{p-3}{2}\right)^{\frac{p-3}{2}} + \left(\frac{p+1}{2}\right)^{\frac{p-1}{2}}\left(\frac{p-1}{2}\right)^{\frac{p-1}{2}} +$$

$$+ \left(\frac{p-3}{2}\right)^{\frac{p-3}{2}}\left(\frac{p-1}{2}\right)^{\frac{p+1}{2}} + \ldots + 2^2 3^{p-3} + 1^1 \cdot 2^{p-2} = 2S_p + \left(\frac{p^2-1}{4}\right)^{\frac{p-1}{2}} \equiv$$

$$\equiv 2S_p + (-1)^{\frac{p-1}{2}} \pmod p,$$

a to smo i hteli da dokažemo.

Na osnovu teoreme 3.2 izlazi da je za $p \in P$, $p \geq 3$

$$!p \equiv 0 \pmod p \Leftrightarrow 2S_p + (-1)^{\frac{p-1}{2}} \equiv 0 \pmod p.$$

No, to znači, da su hipoteze (3.6), odnosno (3.7) ekvivalentne sa hipotezom

$$2S_p + (-1)^{\frac{p-1}{2}} \not\equiv 0 \pmod p, \text{ za svako } p \in P,\ p \geq 3. \tag{3.10}$$

Na žalost, pokušaj da se dokaže ili opovrgne (3.10) nije za sad uspeo, no čini se, da razmatranje kongruencije (3.10) pruža veće šanse na uspeh od razmatranja polazne kongruencije $1+1!+2!+\ldots+(p-1)! \equiv 0 \pmod p$. U svakom slučaju, teoreme 3.1 i 3.2 otvaraju nove mogućnosti za dokazivanje ili obaranje hipoteze Dj.Kurepe o funkciji $!n$.

3.3 Niz polinoma $D_k(x)$

Definišimo sada jedan niz polinoma, koji će kasnije u razmatranju Fermat-ovog problema imati veliku ulogu.

Definicija 3.2 Pod $D_k(x)$, $k \in N$, podrazumevaćemo niz polinoma

$$D_k(x) = \begin{vmatrix} 1 & x & 0 & 0 & \ldots & 0 & 0 \\ 1 & \binom{2}{1} & x & 0 & \ldots & 0 & 0 \\ 1 & \binom{3}{1} & \binom{3}{2} & x & \ldots & 0 & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 1 & \binom{k-2}{1} & \binom{k-2}{2} & \binom{k-2}{3} & \ldots & x & 0 \\ 1 & \binom{k-1}{1} & \binom{k-1}{2} & \binom{k-1}{3} & \ldots & \binom{k-1}{k-2} & x \\ 1 & \binom{k}{1} & \binom{k}{2} & \binom{k}{3} & \ldots & \binom{k}{k-2} & \binom{k}{k-1} \end{vmatrix}. \qquad (3.11)$$

Iz (3.11) se neposredno može izračunati

$D_1(x)=1$, $D_2(x)=2-x$, $D_3(x)=x^2-6x+6$, $D_4(x)=(2-x)(x^2-12x+12)$, ...

Očigledno, radi se o nizu polinoma $k-1$-og stepena. Neka je

$$D_k(x) = a_{k-1,k}x^{k-1} + a_{k-2,k}x^{k-2} + \ldots + a_{1,k}x + a_{0,k} = \sum_{n=1}^{k} a_{k-n,k}x^{k-n}.$$

Utvrdimo neke osnovne osobine definisanog niza

Lema 3.3 Niz $D_k(x)$ zadovoljava rekurentnu formulu

$$(1-x)D_k(x) = D_k(x) - \binom{k}{1}xD_{k-1}(x) + \binom{k}{2}x^2D_{k-2}(x) - \ldots + (-1)^k x^k =$$

$$= \left[D(x) - x\right]^k, \quad k \in N, \qquad (3.12)$$

gde se podrazumeva da je $D^m(x) = D_m(x)$, $m=1,2,\ldots k$.

Dokaz. Razvijajući determinantu (3.11) po elementima poslednje kolone dobijamo

$$D_k(x) = \binom{k}{k-1} D_{k-1}(x) - x \begin{vmatrix} 1 & x & 0 & \dots & 0 & 0 \\ 1 & \binom{2}{1} & x & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 1 & \binom{k-2}{1} & \binom{k-2}{2} & \dots & \binom{k-2}{k-3} & x \\ 1 & \binom{k}{1} & \binom{k}{2} & \dots & \binom{k}{k-3} & \binom{k}{k-2} \end{vmatrix}. \qquad (3.13)$$

Razvijajući determinantu (3.13) po elementima poslednje kolone i ponavljajući taj postupak još $k-2$ puta dobijamo

$$D_k(x) = \binom{k}{k-1} D_{k-1}(x) - \binom{k}{k-2} x D_{k-2}(x) + \binom{k}{k-3} x^2 D_{k-3}(x) - \dots +$$

$$+ (-1)^{k-1} x^{k-1}. \qquad (3.14)$$

Množeći poslednju jednakost sa $-x$ i dodavajući obema stranama $D_k(x)$ izlazi jednakost (3.12). Time je lema u potpunosti dokazana.

Lema 3.4 Koeficijenti $a_{k-n,k}$ zadovoljavaju rekurentnu formulu

$$a_{k-n,k} = \binom{k}{k-1} a_{k-n,k-1} - \binom{k}{k-2} a_{k-n-1,k-2} + \binom{k}{k-3} a_{k-n-2,k-3} - \dots +$$

$$+ (-1)^{k-n} \binom{k}{n-1} a_{0,n-1}, \quad 2 \leqslant n \leqslant k. \qquad (3.15)$$

Dokaz. Na osnovu leme 3.3, uporedjujući u jednakosti (3.14) koeficijente uz x^{k-n}, $2 \leqslant n \leqslant k$, dobijamo neposredno (3.15).

Sada nije teško pokazati da su koeficijenti $a_{k-n,k}$ direktno vezani sa nizom $x_{n,k}$ definisanim u 3.1. Drugim rečima, niz polinoma $D_k(x)$ i niz $x_{n,k}$ čine nerazdvojivu celinu. Dokažimo stoga, sledeću lemu.

Lema 3.5 **Za svako $k \in N$ i svako n, $1 \leqslant n \leqslant k$ važi jednakost**

$$a_{k-n,k} = (-1)^{k-n} x_{n,k} = (-1)^{k-n} [n^k - \binom{n}{1}(n-1)^k + \dots + (-1)^{n-1} \binom{n}{n-1} 1^k]. \qquad (3.16)$$

Dokaz. **Lemu ćemo da dokažemo metodom matematičke indukcije po k. Za $k=1$, mora biti $n=1$, pa je tvrdjenje tačno, jer je**

$$a_{0,1} = 1 = (-1)^{1-1} x_{1,1}.$$

Pretpostavimo da je (3.16) tačno za svako $k=1,2,\dots m-1$ i svako n, $1 \leqslant n \leqslant k$. Dokažimo da je (3.16) tačno za prirodan broj m i svako n,

$1 \leq n \leq m$.

Za $n=1$ iz (3.14) dobijamo direktno

$$a_{m-1,m} = (-1)^{m-1} = (-1)^{m-1} x_{1,m}.$$

Za $2 \leq n \leq m$, na osnovu (3.15), koristeći induktivnu pretpostavku dobijamo

$$a_{m-n,m} = \binom{m}{m-1} a_{m-1-(n-1),m-1} - \binom{m}{m-2} a_{m-2-(n-1),m-2} + \ldots +$$

$$+ (-1)^{m-n} \binom{m}{n-1} a_{n-1-(n-1),n-1} = \binom{m}{m-1} (-1)^{m-n} x_{n-1,m-1} -$$

$$- \binom{m}{m-2} (-1)^{m-n-1} x_{n-1,m-2} + \ldots + (-1)^{m-n} \binom{m}{n-1} (-1)^{0} x_{n-1,n-1} =$$

$$= (-1)^{m-n} \left[\binom{m}{m-1} \left[(n-1)^{m-1} - \binom{n-1}{1} (n-2)^{m-1} + \binom{n-1}{2} (n-3)^{m-1} - \ldots + \right. \right.$$

$$\left. + (-1)^{n-2} \binom{n-1}{n-2} \right] + \binom{m}{m-2} \left[(n-1)^{m-2} - \binom{n-1}{1} (n-2)^{m-2} + \binom{n-1}{2} (n-3)^{m-2} - \right.$$

$$\left. - \ldots + (-1)^{n-2} \binom{n-1}{n-2} \right] + \ldots + \binom{m}{n-1} \left[(n-1)^{n-1} - \binom{n-1}{1} (n-2)^{n-1} + \right.$$

$$\left. + \binom{n-1}{2} (n-3)^{n-1} - \ldots + (-1)^{n-2} \binom{n-1}{n-2} \right] = (-1)^{m-n} \left[\left[\binom{m}{m-1} (n-1)^{m-1} + \right. \right.$$

$$+ \binom{m}{m-2} (n-1)^{m-2} + \ldots + \binom{m}{n-1} (n-1)^{n-1} \left. \right] - \binom{n-1}{1} \left[\binom{m}{m-1} (n-2)^{m-1} + \right.$$

$$+ \binom{m}{m-2} (n-2)^{m-2} + \ldots + \binom{m}{n-1} (n-2)^{n-1} \left. \right] + \binom{n-1}{2} \left[\binom{m}{m-1} (n-3)^{m-1} + \right.$$

$$+ \binom{m}{m-2} (n-3)^{m-2} + \ldots + \binom{m}{n-1} (n-3)^{n-1} \left. \right] - \ldots +$$

$$\left. + (-1)^{n-2} \binom{n-1}{n-2} \left[\binom{m}{m-1} 1^{m-1} + \binom{m}{m-2} 1^{m-2} + \ldots + \binom{m}{n-1} 1^{n-1} \right] \right] =$$

$$= (-1)^{m-n} \left[\left[((n-1)+1)^{m} - (n-1)^{m} - \left(\binom{m}{n-2} (n-1)^{n-2} + \ldots + \binom{m}{1} (n-1) + \right. \right. \right.$$

$$\left. + 1) \right] - \binom{n-1}{1} \left[((n-2)+1)^{m} - (n-2)^{m} - \left(\binom{m}{n-2} (n-2)^{n-2} + \ldots + \right. \right.$$

$$\left. + \binom{m}{1} (n-2) + 1) \right] + \binom{n-1}{2} \left[((n-3)+1)^{m} - (n-3)^{m} - \left(\binom{m}{n-2} (n-3)^{n-2} + \right. \right.$$

$$\left. + \ldots + \binom{m}{1} (n-3) + 1) \right] - \ldots + (-1)^{n-2} \binom{n-1}{n-2} \left[(1+1)^{m} - 1^{m} - \right.$$

$$\left. - \left(\binom{m}{n-2} 1^{n-2} + \ldots + \binom{m}{1} 1 + 1) \right] \right] = (-1)^{m-n} \left[\left[n^{m} - \left(\binom{n-1}{0} + \right. \right. \right.$$

$$+ \binom{n-1}{1} \Big) (n-1)^{m} + \left(\binom{n-1}{1} + \binom{n-1}{2} \right) (n-2)^{m} - \ldots + (-1)^{n-2} \left(\binom{n-1}{n-3} + \binom{n-1}{n-2} \right) 2^{m} +$$

$$\left. + (-1)^{n-1} \binom{n-1}{n-2} 1^{m} \right] - \binom{m}{n-2} \left[(n-1)^{n-2} - \binom{n-1}{1} (n-2)^{n-2} + \binom{n-1}{2} (n-3)^{n-2} - \right.$$

$$\left. - \ldots + (-1)^{n-2} \binom{n-1}{n-2} 1^{n-2} \right] - \ldots - \binom{m}{1} \left[(n-1) - \binom{n-1}{1} (n-2) + \right.$$

$$+ \binom{n-1}{2}(n-3) - \ldots + \binom{n-1}{n-2}1] - [1 - \binom{n-1}{1} + \binom{n-1}{2} - \ldots +$$

$$+ (-1)^{n-2}\binom{n-1}{n-2}]\Big] = (-1)^{m-n}\Big[[n^m - \binom{n}{1}(n-1)^m + \binom{n}{2}(n-2)^m - \ldots +$$

$$+ (-1)^{n-2}\binom{n}{n-2}2^m + (-1)^{n-1}\binom{n-1}{n-2}] - \binom{m}{n-2}x_{n-1,n-2} - \binom{m}{n-3}x_{n-1,n-3} -$$

$$- \ldots - \binom{m}{1}x_{n-1,1} + (-1)^{n-1}\Big].$$

Na osnovu leme 3.1, važi

$$x_{n-1,n-2} = x_{n-1,n-3} = \ldots = x_{n-1,1} = 0,$$

pa konačno dobijamo

$$a_{m-n,m} = (-1)^{m-n}[(x_{n,m} - (-1)^{n-1}) + (-1)^{n-1}] = (-1)^{m-n}x_{n,m}.$$

Dakle, iz pretpostavke da je tvrdjenje tačno za svako $k=1,2,\ldots m-1$ i svako r, $1\leqslant n\leqslant k$, dokazali smo da je tvrdjenje tačno za $k=m$ i svako n, $1\leqslant n\leqslant m$, pa kako je tvrdjenje tačno i za $k=1=n$, to prema principu matematičke indukcije zaključujemo da je tvrdjenje tačno za svako $k\in N$ i svako n, $1\leqslant n\leqslant k$. Time je lema u potpunosti dokazana.

Kao prva posledica leme 3.5 proizilazi lema 3.2, odnosno jednakost (3.3). Naime, iz (3.11) je jasno da je slobodan član $a_{o,k}$ polinoma $D_k(x)$

$$a_{o,k} = 1\binom{2}{1}\binom{3}{2}\ldots\binom{k}{k-1} = k!,$$

a prema lemi 3.5 je

$$a_{o,k} = x_{k,k} = k^k - \binom{k}{1}(k-1)^k + \ldots + (-1)^{k-1}\binom{k}{k-1}1^k.$$

Sad se nameće ideja da računajući determinantu $D_k(x)$ po definiciji možemo doći do sličnih jednakosti za $x_{n,k}$, $1\leqslant n\leqslant k-1$. Drugim rečima, sada smo u stanju da dokažemo jednakost (3.4), tj. da dokažemo osobinu 1^o niza $x_{n,k}$.

Teorema 3.3 Neka je $1\leqslant j\leqslant k-n$ i neka je N_j odredjeno sa

$$N_j = \sum\Big[\prod_{l=1}^{s}\alpha_l!\,[(m_l+1)!]^{\alpha_l}\Big]^{-1},$$

gde se sumiranje vrši po svim slučajevima kada je $s\geqslant 1$, $\alpha_1+\alpha_2+\ldots+\alpha_s=j$, $1\leqslant\alpha_1\leqslant\alpha_2\leqslant\ldots\leqslant\alpha_s$, $m_1\alpha_1+m_2\alpha_2+\ldots+m_s\alpha_s=k-n$,

$m_i \neq m_l$, $\alpha_i = \alpha_l \Rightarrow m_i < m_l$. Tada je

$$x_{n,k} = k! \sum_{j=1}^{k-n} \binom{n}{j} j! N_j, \quad n \leqslant k-1. \tag{3.17}$$

Dokaz. Prema lemi 3.5 važi $a_{k-n,k} = (-1)^{k-n} x_{n,k}$. Da dokažemo teoremu izračunajmo $D_k(x)$ po definiciji i ustanovimo koji se koeficijent nalazi uz x^{k-n}, $1 \leqslant n \leqslant k-1$.

Uočimo sledeće. Neka iz prvih $i-1$ vrste nije izabrana nijedna 0 i neka iz $i-1$-ve vrste nije izabran x. Razlikujmo dva slučaja:

1° Iz i-te vrste nije izabran ni x ni 0. Pokažimo da u i-toj vrsti mora biti izabran element $\binom{i}{i-1} = i$. Stvarno, iz prvih i kolona u prvih $i-1$ vrsta izabrano je po pretpostavci $i-1$ elemenata; znači, ostala je samo jedna kolona iz koje nije izabran nijedan element. Za izbor u i-toj vrsti imamo ili x, ili 0, ili element iz te, pomenute kolone. Kako iz $i-1$-ve vrste nije izabran x, to iz i-te kolone nije do sad izabran nijedan element, pa sledi da u i-toj vrsti mora biti izabran $\binom{i}{i-1}$.

2° Iz i-te, $i+1$-ve,..., $i+r-1$-ve vrste je izabran x, a iz $i+r$-te nije izabran ni x, ni 0, $r \geqslant 1$. Pokažimo da iz $i+r$-te vrste mora biti izabran element $\binom{i+r}{i-1}$. Stvarno, iz prvih $i+r$ kolona izabrano je u prvih $i+r-1$ vrsta tačno $i+r-1$ element. Dakle, iz jedne jedine kolone nije izabran nijedan element. Za izbor u $i+r$-toj vrsti imamo 0, x ili element iz te, pomenute kolone. Po pretpostavci iz i-te kolone nije izabran do sad nijedan element, pa u $i+r$-toj vrsti moramo da izaberemo $\binom{i+r}{i-1}$.

Uočimo sad u razvoju determinante $D_k(x)$ jedan od monoma koji sadrže x^{k-n}. Očigledno, koeficijent uz njega zavisi od toga kako je izabrano tih $k-n$ x-eva. Neka je izbor bio takav da je napravljeno j grupa, $1 \leqslant j \leqslant k-n$, pri čemu pod jednom grupom podrazumevamo da je izvestan broj x uzet iz susednih vrsta. Grupe se razlikuju po dužini; neka je α_1 dužine m_1, α_2 dužine m_2,..., α_s dužine m_s, $s \geqslant 1$, $1 \leqslant \alpha_1 \leqslant \alpha_2 \leqslant \ldots \leqslant \alpha_s$, $m_i \neq m_l$, $\alpha_i = \alpha_l \Rightarrow m_i < m_l$. Očigledno, mora biti

$$\alpha_1 + \alpha_2 + \ldots + \alpha_s = j, \quad \alpha_1 m_1 + \alpha_2 m_2 + \ldots + \alpha_s m_s = k - n.$$

Neka su dalje $k_1, k_2, \ldots, k_j$ dužine uočenih j grupa, pri čemu je k_1 dužina grupe smeštene u vrstama sa najmanjim indeksom, k_2 dužina

sledeće,..., k_s dužina grupe smeštene u vrstama sa najvećim indeksom.

Primenjujući malopredjašnje rasudjivanje, izlazi da je koeficijent uz x^{k-n}

$$(-1)^r 1\ldots(i_1-1)\binom{i_1+k_1}{i_1-1}(i_1+k_1+1)\ldots(i_2-1)\binom{i_2+k_2}{i_2-1}(i_2+$$

$$+k_2+1)\ldots(i_j-1)\binom{i_j+k_j}{i_j-1}(i_j+k_j+1)\ldots k =$$

$$=(-1)^r 1\ldots(i_1-1)\binom{i_1+k_1}{k_1+1}(i_1+k_1+1)\ldots(i_2-1)\binom{i_2+k_2}{k_2+1}(i_2+$$

$$+k_2+1)\ldots(i_j-1)\binom{i_j+k_j}{k_j+1}(i_j+k_j+1)\ldots k =$$

$$=(-1)^r k!\prod_{m=1}^{j}[(k_m+1)!]^{-1}.$$

Kako po pretpostavci medju dužinama $k_1,k_2,\ldots k_j$.ima α_1 dužine m_1, α_2 dužine $m_2,\ldots,$ α_s dužine m_s, to izlazi da je koeficijent kod uočenog monoma

$$(-1)^r k!\prod_{l=1}^{s}[(m_l+1)!]^{-\alpha_l}.$$

Ostaje još odredjivanje znaka kod uočenog monoma. Očigledno se radi o permutaciji

$$1\ \ldots\ i_1-1\ i_1+1\ \ldots\ i_1+k_1\ i_1\ i_1+k_1+1\ \ldots\ k,$$

u kojoj je napravljeno ukupno r inverzija, tj.

$$r=k_1+k_2+\ldots+k_j=m_1\alpha_1+m_2\alpha_2+\ldots+m_s\alpha_s=k-n.$$

Dakle, konačno, koeficijent uočenog monoma glasi

$$(-1)^{k-n}k!\prod_{l=1}^{s}[(m_l+1)!]^{-\alpha_l}. \qquad (3.18)$$

Problem se konačno sveo na to, da se odredi koliko takvih monoma ima. Drugim rečima, problem se sveo na kombinatorni problem: Na koliko se načina iz $k-1$ vrste može izabrati $k-n$ x-eva, tako da ovi formiraju tačno j grupa, $1\leqslant n\leqslant k-1$, $1\leqslant j\leqslant k-n$. Jasno, svaka od postojećih kombinacija ima svoju "težinu" (3.18).

Izaberimo iz svake grupe po jednog predstavnika i numerišimo ga sa $m_1, m_2, \ldots, m_s$, odnosno, neka numeracija predstavlja dužinu grupe iz koje je izabran. Postavljeni problem ekvivalentan je sad problemu: na koliko se načina može j numerisanih predstavnika rasporediti na $(k-1)-[(k-n)-j]=n+j-1$ mesto, s tim da dva predstavnika nisu jedan do drugog. Pošto j predstavnika, na taj način rasporedjenih, zauzimaju $j+(j-1)=2j-1$ mesto, to je ovaj problem ekvivalentan problemu, na koliko se načina može j označenih predstavnika (medju kojima ima α_1 jednakih, pa α_2 jednakih, ... , pa α_s jednakih) rasporediti na $(n+j-1)-(j-1)=n$ mesta. To je očigledno moguće učiniti na

$$\binom{n}{j} \frac{j!}{\alpha_1!\alpha_2!\ldots\alpha_s!}\ ,\ \alpha_1+\alpha_2+\ldots+\alpha_s=j,$$

načina. Uzimajući u obzir (3.18), izlazi definitivno

$$a_{k-n,k}=(-1)^{k-n}x_{n,k}=\sum_{j=1}^{k-n}\sum\binom{n}{j}\frac{j!}{\alpha_1!\alpha_2!\ldots\alpha_s!}\times$$

$$\times(-1)^{k-n}k!\prod_{l=1}^{s}[(m_l+1)!]^{-\alpha_l}=(-1)^{k-n}k!\sum_{j=1}^{k-n}\binom{n}{j}j!N_j,$$

a to smo i trebali da dokažemo.

Teorema 3.3 nam, izmedju ostalog, omogućuje da biramo način izračunavanja koeficijenata $a_{k-n,k}$ polinoma $D_k(x)$. Jasno je da će za vrednosti n koje se malo razlikuju od k, biti neuporedivo lakše računati $a_{k-n,k}$ preko teoreme 3.3, odnosno jednakosti (3.17), nego preko leme 3.5, odnosno jednakosti (3.16). Primenimo teoremu 3.3 na $n=k-1, k-2, \ldots, k-8$.

Neka je $n=k-1$. Tu je $k-n=1$, $j=1$, $s=1$, $\alpha_1=m_1=1$. Izlazi primenom (3.17)

$$a_{1,k}=-x_{k-1,k}=-k!\binom{k-1}{1}1!\ \frac{1}{1!2!}=-\frac{k!}{2}\binom{k-1}{1}. \qquad (3.19)$$

Neka je $n=k-2$. Tu je $k-n=2$, $j=1,2$. Za $j=1$ izlazi $\alpha_1=1$, $m_1=2$, a za $j=2$, $\alpha_1=2$, $m_1=1$, pa (3.17) daje

$$a_{2,k}=x_{k-2,k}=k!\left[\binom{k-2}{1}1!\ \frac{1}{1!3!}+\binom{k-2}{2}2!\ \frac{1}{2!(2!)^2}\right]=$$

$$= \frac{k!}{2\cdot 3!}\left[3\binom{k-2}{2}+2\binom{k-2}{1}\right]. \qquad (3.20)$$

Neka je $n=k-3$. Tu je $k-n=3$, $1\leqslant j\leqslant 3$. Za $j=1$, $\alpha_1=1$, $m_1=3$; za $j=2$, $\alpha_1=\alpha_2=1$, $m_1=1$, $m_2=2$; za $j=3$, $\alpha_1=3$, $m_1=1$. Dobijamo

$$a_{3,k}=-x_{k-3,k}=-k!\left[\binom{k-3}{1}1!\,\frac{1}{1!4!}+\binom{k-3}{2}2!\,\frac{1}{1!1!2!3!}+\right.$$

$$\left.+\binom{k-3}{3}3!\,\frac{1}{3!(2!)^3}\right]=-\frac{k!}{4!}\left[3\binom{k-3}{3}+4\binom{k-3}{2}+\binom{k-3}{1}\right]. \qquad (3.21)$$

Neka je $n=k-4$. Tu je $k-n=4$, $1\leqslant j\leqslant 4$. Za $j=1$, $\alpha_1=1$, $m_1=4$; za $j=2$, $\alpha_1=2$, $m_1=2$, ili $\alpha_1=1$ $\alpha_2=1$, $m_1=1$, $m_2=3$; za $j=3$, $\alpha_1=1$, $\alpha_2=2$, $m_1=2$, $m_2=1$; za $j=4$, $\alpha_1=4$, $m_1=1$. Dobijamo

$$a_{4,k}=x_{k-4,k}=k!\left[\binom{k-4}{1}1!\,\frac{1}{1!5!}+\binom{k-2}{2}2!\left(\frac{1}{2!(3!)^2}+\right.\right.$$

$$\left.\left.+\frac{1}{1!1!2!3!}\right)+\binom{k-4}{3}3!\,\frac{1}{1!2!3!(2!)^2}+\binom{k-4}{4}4!\,\frac{1}{(2!)^4 4!}\right]=$$

$$=\frac{k!}{6!}\left[45\binom{k-4}{4}+90\binom{k-4}{3}+50\binom{k-4}{2}+6\binom{k-4}{1}\right]. \qquad (3.22)$$

Analogno računajući dalje, nakon sredjivanja izlazi

$$a_{5,k}=-x_{k-5,k}=-\frac{k!}{2\cdot 6!}\left[45\binom{k-5}{5}+120\binom{k-5}{4}+105\binom{k-5}{3}+\right.$$

$$\left.+32\binom{k-5}{2}+2\binom{k-5}{1}\right], \qquad (3.23)$$

$$a_{6,k}=x_{k-6,k}=\frac{k!}{12\cdot 7!}\left[945\binom{k-6}{6}+3150\binom{k-6}{5}+3780\binom{k-6}{4}+\right.$$

$$\left.+1918\binom{k-6}{3}+357\binom{k-6}{2}+12\binom{k-6}{1}\right], \qquad (3.24)$$

$$a_{7,k}=-x_{k-7,k}=-\frac{k!}{3\cdot 8!}\left[945\binom{k-7}{7}+3780\binom{k-7}{6}+5775\binom{k-7}{5}+\right.$$

$$\left.+4144\binom{k-7}{4}+1365\binom{k-7}{3}+164\binom{k-7}{2}+3\binom{k-7}{1}\right], \qquad (3.25)$$

$$a_{8,k}=x_{k-8,k}=\frac{k!}{10!}\left[14175\binom{k-8}{8}+66150\binom{k-8}{7}+122850\binom{k-8}{6}+\right.$$

$$+114450\binom{k-8}{5}+55090\binom{k-8}{4}+12510\binom{k-8}{3}+1002\binom{k-8}{2}+$$

$$\left.+10\binom{k-8}{1}\right]. \qquad (3.26)$$

3.4 Dalje osobine niza $D_k(x)$

Niz polinoma $D_k(x)$ igraće kasnije u razmatranju Fermat-ovog problema vidnu ulogu. To opravdava naš trud da uočimo još neke, inače same za sebe interesantne, osobine ovog niza. Dokažimo, pre svega, jednu pomoćnu lemu.

Lema 3.6 Neka je $A_{j,k}(x)$, $0 \leqslant j \leqslant k-1$, niz polinoma definisan na sledeći način

$$A_{j,k}(x) = \begin{vmatrix} \binom{j+1}{j} & x & 0 & 0 & \dots & 0 & 0 \\ \binom{j+2}{j} & \binom{j+2}{j+1} & x & 0 & \dots & 0 & 0 \\ \binom{j+3}{j} & \binom{j+3}{j+1} & \binom{j+3}{j+2} & x & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ \binom{k-1}{j} & \binom{k-1}{j+1} & \binom{k-1}{j+2} & \binom{k-1}{j+3} & \dots & \binom{k-1}{k-2} & x \\ \binom{k}{j} & \binom{k}{j+1} & \binom{k}{j+2} & \binom{k}{j+3} & \dots & \binom{k}{k-2} & \binom{k}{k-1} \end{vmatrix}. \qquad (3.27)$$

Tada je

$$A_{j,k}(x) = \binom{k}{j} D_{k-j}(x). \qquad (3.28)$$

Dokaz. Pomnožimo determinantu $A_{j,k}(x)$ sa $j!(j+1)!\dots(k-1)!$ i to tako, da prvu kolonu pomnožimo sa $j!$, drugu sa $(j+1)!,\dots,$ $(k-j)$-tu sa $(k-1)!$. Dobijamo

$$A_{j,k}(x) = \prod_{i=j}^{k-1} (i!)^{-1} = \begin{vmatrix} \frac{(j+1)!}{1!} & x(j+1)! & 0 & \dots & 0 & 0 \\ \frac{(j+2)!}{2!} & \frac{(j+2)!}{1!} & x(j+2)! & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ \frac{k!}{(k-j)!} & \frac{k!}{(k-j-1)!} & \frac{k!}{(k-j-2)!} & \dots & \frac{k!}{2!} & \frac{k!}{1!} \end{vmatrix} =$$

$$= \frac{k!}{j!} \begin{vmatrix} \frac{1}{1!} & x & 0 & \dots & 0 & 0 \\ \frac{1}{2!} & \frac{1}{1!} & x & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ \frac{1}{(k-j)!} & \frac{1}{(k-j-1)!} & \frac{1}{(k-j-2)!} & \dots & \frac{1}{2!} & \frac{1}{1!} \end{vmatrix}.$$

Ako poslednju determinantu pomnožimo sa $1!2!\ldots(k-j)!$ i to tako, da prvu vrstu pomnožimo sa $1!$, drugu sa $2!,\ldots,$ $(k-j)$-tu sa $(k-j)!$, dobijamo

$$A_{j,k}(x) = k!\left[j!\prod_{i=1}^{k-j} i!\right]^{-1}\begin{vmatrix} 1 & x1! & 0 & \ldots & 0 & 0 \\ 1 & \frac{2!}{1!} & x2! & \ldots & 0 & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 1 & \frac{(k-j)!}{(k-j-1)!} & \frac{(k-j)!}{(k-j-2)!} & \ldots & \frac{(k-j)!}{2!} & \frac{(k-j)!}{1!} \end{vmatrix} =$$

$$= \frac{k!}{(k-j)!j!}\begin{vmatrix} 1 & x & 0 & \ldots & 0 & 0 \\ 1 & \frac{2!}{1!1!} & x & \ldots & 0 & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 1 & \frac{(k-j)!}{(k-j-1)!1!} & \frac{(k-j)!}{(k-j-2)!2!} & \ldots & \frac{(k-j)!}{2!(k-j-2)!} & \frac{(k-j)!}{1!(k-j-1)!} \end{vmatrix} =$$

$$= \binom{k}{j} D_{k-j}(x),$$

a to smo i hteli da dokažemo.

Sada smo u mogućnosti da izvedemo još jednu rekurentnu formulu niza $D_k(x)$.

Lema 3.7 Za niz $D_k(x)$ važi

$$D_k(x) = (1-x)\left[D(x)+x\right]^k + x^{k+1}, \qquad (3.29)$$

gde se podrazumeva da je $D^m(x) = D_m(x)$, $m=1,2,\ldots,k$.

Dokaz. Neka je m proizvoljan broj. Dodajmo prvoj koloni determinante $D_k(x)$ drugu pomnoženu sa m, treću pomnoženu sa $m^2,\ldots,$ k-tu pomnoženu sa m^{k-1}. Element u i-toj vrsti, prvoj koloni, dobijene determinante je

$$1 + \binom{i}{1}m + \binom{i}{2}m^2 + \ldots + \binom{i}{i-1}m^{i-1} + xm^i = (1+m)^i + m^i(x-1), \quad 1\leqslant i\leqslant k-1,$$

$$1 + \binom{k}{1}m + \binom{k}{2}m^2 + \ldots + \binom{k}{k-1}m^{k-1} = (1+m)^k + m^k(x-1) - m^k x, \quad i=k.$$

Drugim rečima, važi

$$D_k(x) = \begin{vmatrix} (1+m)+m(x-1) & x & 0 & \ldots & 0 \\ (1+m)^2 + m^2(x-1) & \binom{2}{1} & x & \ldots & 0 \\ (1+m)^3 + m^3(x-1) & \binom{3}{1} & \binom{3}{2} & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ (1+m)^{k-1} + m^{k-1}(x-1) & \binom{k-1}{1} & \binom{k-1}{2} & \ldots & x \\ (1+m)^k + m^k(x-1) - m^k x & \binom{k}{1} & \binom{k}{2} & \ldots & \binom{k}{k-1} \end{vmatrix}. \qquad (3.30)$$

Stavljajući u (3.30) $m=-1$ i rastavljajući determinantu na zbir dve determinante izlazi

$$D_k(x) = (1-x)\begin{vmatrix} 1 & x & 0 & \dots & 0 \\ -1 & \binom{2}{1} & x & \dots & 0 \\ 1 & \binom{3}{1} & \binom{3}{2} & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ (-1)^{k-2} & \binom{k-1}{1} & \binom{k-1}{2} & \dots & x \\ (-1)^{k-1} & \binom{k}{1} & \binom{k}{2} & \dots & \binom{k}{k-1} \end{vmatrix} +$$

$$+ \begin{vmatrix} 0 & x & 0 & \dots & 0 \\ 0 & \binom{2}{1} & x & \dots & 0 \\ 0 & \binom{3}{1} & \binom{3}{2} & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & \binom{k-1}{1} & \binom{k-1}{2} & \dots & x \\ (-1)^{k-1}x & \binom{k}{1} & \binom{k}{2} & \dots & \binom{k}{k-1} \end{vmatrix} . \qquad (3.31)$$

Druga, od dve determinante u jednakosti (3.31), je očigledno jednaka x^k. Prvu pak, razvijmo po elementima prve kolone, imajući u vidu lemu 3.6, odnosno jednakost (3.28). Dobijamo

$$D_k(x) = (1-x)\left[A_{1,k}(x) + xA_{2,k}(x) + \dots + x^{k-2}A_{k-1,k}(x) + x^{k-1}\right] + x^k = (1-x)\left[\binom{k}{1}D_{k-1}(x) + \binom{k}{2}xD_{k-2}(x) + \dots + \binom{k}{k-1}x^{k-2}D_1(x) + x^{k-1}\right] + x^k.$$

Pomnožimo li poslednju jednakost sa x i dodamo li obema stranama $(1-x)D_k(x)$, izlazi jednakost (3.29). Time je lema u potpunosti dokazana.

Prva posledica leme 3.7 je osobina 3° niza $x_{n,k}$, iznета u 3.1. Naime, stavljajući u (3.29) $x=1$, izlazi $D_k(1)=1$. Drugim rečima, važi sledeća lema.

Lema 3.8 Za svako $k \in N$ važi jednakost

$$D_k(1) = \sum_{n=1}^{k} (-1)^{k-n} x_{n,k} = 1. \qquad (3.32)$$

Sledeća posledica leme 3.7 biće za nas još značajnija.

Lema 3.9 Za svako $k \in N$ važi jednakost

$$D_k(x) = (1-x)^{k-1} D_k\left(\frac{x}{x-1}\right), \quad x \neq 1. \qquad (3.33)$$

Dokaz. Lemu ćemo da dokažemo matematičkom indukcijom. Za $k=1$ tvrdjenje je tačno, jer je

$$D_1(x) = D_1\left(\frac{x}{x-1}\right) = 1, \quad x \neq 1.$$

Pretpostavimo da je jednakost (3.33) tačna za svako $k=1,2,\ldots,m-1$, $m \geq 2$, i dokažimo da je (3.33) tačno za $k=m$.

Za $x=o$ jednakost (3.33) je očigledno tačna. Neka je $x \neq 0$, $x \neq 1$. Stavljajući u jednakost (3.12), umesto x, $\frac{x}{x-1}$ dobijamo za $k=m$

$$\left(1 - \frac{x}{x-1}\right) D_m\left(\frac{x}{x-1}\right) = \left[D\left(\frac{x}{x-1}\right) - \frac{x}{x-1}\right]^m =$$

$$= (x-1)^{-m}\left[(x-1)^m D_m\left(\frac{x}{x-1}\right) - \binom{m}{1} x(x-1)^{m-1} D_{m-1}\left(\frac{x}{x-1}\right) + \ldots +\right.$$

$$\left. + (-1)^{m-1}\binom{m}{m-1} x^{m-1}(x-1) D_1\left(\frac{x}{x-1}\right) + (-1)^m x^m\right] =$$

$$= (1-x)^{1-m}\left[(1-x)^{m-1} D_m\left(\frac{x}{x-1}\right) + \binom{m}{1} x(1-x)^{m-2} D_{m-1}\left(\frac{x}{x-1}\right) +\right.$$

$$\left. + \ldots + \binom{m}{m-1} x^{m-1} D_1\left(\frac{x}{x-1}\right)\right] + x^m(1-x)^{-m}. \qquad (3.34)$$

Koristeći induktivnu pretpostavku, imajući na umu (3.29), iz (3.34) sledi

$$\frac{x}{1-x} D_m\left(\frac{x}{x-1}\right) = (1-x)^{1-m}\left[\binom{m}{1} x D_{m-1}(x) + \binom{m}{2} x^2 D_{m-2}(x) +\right.$$

$$\left. + \ldots + \binom{m}{m-1} x^{m-1} D_1(x)\right] + x^m(1-x)^{-m} =$$

$$= (1-x)^{1-m}\left[(D(x)+x)^m - D_m(x) - x^m\right] + x^m(1-x)^{-m} =$$

$$= (1-x)^{1-m}\left[(D_m(x)-x^{m+1})(1-x)^{-1} - D_m(x) - x^m\right] +$$

$$+ x^m(1-x)^{-m} = (1-x)^{-m} x D_m(x),$$

odnosno, nakon sredjivanja

$$D_m(x) = (1-x)^{m-1} B_m\left(\frac{x}{x-1}\right).$$

Dakle, iz pretpostavke da je jednakost (3.33) tačna za svako $k=1,2,\ldots,m-1$, $m\geq 2$, dokazali smo da je (3.33) tačno za $k=m$, pa kako je (3.33) tačno i za $k=1$, to zaključujemo da je (3.33) tačno za svako $k \in N$.

Prirodno je da, razratrajući niz polinoma $D_k(x)$, postavimo pitanja vezana za nule polinoma $D_k(x)$. Sledeće tri leme daju odgovor na ta pitanja. Osim toga, prva od njih, dokazuje osobinu 2° niza $x_{n,k}$, iznetu u 3.1.

Lema 3.10 Za svako $k \in N$ je $D_k(2)=0$ ako i samo ako je k parno.

Dokaz. Neka je k parno. Na osnovu leme 3.9, stavljajući u (3.33) $x=2$, dobijamo

$$D_k(2) = (-1)^{k-1} D_k(2) = - D_k(2) \Rightarrow D_k(2) = 0.$$

Da dokažemo obrnuto tvrdjenje, dokažimo prvo da je za svako $k \in N$ i svako $n\geq 3$

$$x_{n,k} \equiv 0 \pmod 3. \qquad (3.35)$$

Za $k=1$ tvrdjenje je tačno, jer je $x_{n,1} = 0$, $n\geq 3>1$. Pretpostavimo da je tvrdjenje tačno za neko $k-1$, $k\geq 2$, i svako $n\geq 3$. Tada na osnovu (3.2) izlazi za $n\geq 4$, $n-1\geq 3$

$$x_{n,k} = n(x_{n,k-1} + x_{n-1,k-1}) \equiv 0 \pmod 3.$$

Za $n=3$ je

$$x_{3,k} = 3^k - \binom{3}{1}2^k + \binom{3}{2}1^k \equiv 0 \pmod 3.$$

Time je matematičkom indukcijom dokazano da za svako $k \in N$ i svako $n\geq 3$ važi (3.35).

Na osnovu leme 3.5, iz (3.35) sledi

$$D_k(x) \equiv (-1)^{k-1}x^{k-1} + (-1)^{k-2}a_{k-2,k}x^{k-2} = (-1)^{k-1}x^{k-1} + (-1)^{k-2}(2^k - 2)x^{k-2} \pmod 3. \qquad (3.36)$$

Neka je sad $D_k(2)=0$. Dokažimo da k mora biti parno. Pretpostavimo obrnuto, neka je k neparno. Tada je

$$2^k - 2 \equiv 0 \pmod 3,$$

pa iz (3.36) sledi za $x=2$

$$D_k(2) \equiv 2^{k-1} \not\equiv 0 \pmod 3,$$

što protivreči pretpostavci da je $D_k(2)=0$. Znači,

$$D_k(2) = 0 \Rightarrow k \text{ je parno.}$$

Time je lema u potpunosti dokazana.

Lema 3.11 Za svako $k \in N$ polinom $D_k(x)$ nema racionalne nule, izuzev nule $x=2$ za k parno.

Dokaz. Na osnovu leme 3.10, potrebno je dokazati da za $x \neq 2$ polinom $D_k(x)$ nema racionalne nule.

Prema poznatom stavu iz teorije polinoma, ako je $\frac{p}{q}$ racionalni koren polinoma

$$b_o x^n + b_1 x^{n-1} + \ldots + b_n, \quad p \in D, \quad q \in N, \quad (p,q)=1,$$

tada je

$$b_o \equiv 0 \pmod q, \quad b_n \equiv 0 \pmod p.$$

Najstariji koeficijent polinoma $D_k(x)$ je $(-1)^{k-1}$, pa ako je $\frac{p}{q}$ racionalni koren polinoma $D_k(x)$, mora biti $q=1$. No, prema lemi 3.9, ako je $\frac{p}{1} = p$ koren polinoma $D_k(x)$, tada je i $\frac{p}{p-1}$ koren tog polinoma. Sledi $p-1=1$, odnosno $p=2$. Znači, izuzev eventualno nule $x=2$, polinom $D_k(x)$ nema racionalnih nula, što smo i hteli da dokažemo.

Lema 3.12 Za svako $k>2$ polinom $D_k(x)$ ima sve nule realne i jednostruke. Pri tom je $[\frac{k-1}{2}]$ nula u intervalu $(1,2)$, a $[\frac{k-1}{2}]$ nula u intervalu $(2,+\infty)$. (Za k parno preostala nula je $x=2$.)

Dokaz. Kako je $D_k(0) = k! \neq 0$, to u daljem razmatranju možemo bez ograničenja pretpostaviti da je $x \neq 0$. Posmatrajmo polinom $F_k(x) = x^{k-1} D_k(\frac{1}{x})$. Prema lemi 3.5 je

$$F_k(x) = \sum_{n=1}^{k} (-1)^{k-n} x_{n,k} x^{n-1}. \tag{3.37}$$

Prema (3.2) važi

$$x_{n,k} = n(x_{n,k-1} - x_{n-1,k-1}), \quad n>2, \quad k>2. \tag{3.38}$$

Iz (3.37) i (3.38), vodeći računa da je prema lemi 3.1 $x_{n,k} = 0$ za svako $n>k$, dobijamo za $k>2$

$$F_k(x) = (-1)^{k-1} + \sum_{n=2}^{k} (-1)^{k-n} n(x_{n,k-1} + x_{n-1,k-1}) x^{n-1} =$$

$$= (-1)^{k-1} + \left[\sum_{n=2}^{k} (-1)^{k-n}(x_{n,k-1} + x_{n-1,k-1})x^n\right]' =$$

$$= (-1)^{k-1} + \left[-x\sum_{n=2}^{k-1} (-1)^{k-1-n}x_{n,k-1}x^{n-1}\right]' +$$

$$+ \left[x^2\sum_{n=2}^{k} (-1)^{k-n}x_{n-1,k-1}x^{n-2}\right]' = (-1)^{k-1} + [-x(F_{k-1}(x) -$$

$$- (-1)^{k-2})]' + [x^2F_{k-1}(x)]' = [(x^2 - x)F_{k-1}(x)]' . \quad (3.39)$$

Pokažimo sad matematičkom indukcijom po k, $k\geq 2$, da polinom $F_k(x)$ ima sve nule realne i jednostruke, pri čemu sve pripadaju intervalu $(0,1)$. Za $k=2$, tvrdjenje je tačno, jer je

$$F_2(x) = xD_2(\frac{1}{x}) = 2x - 1.$$

Pretpostavimo da je tvrdjenje tačno za neki prirodan broj $k-1$, $k\geq 3$, i dokažimo da je tvrdjenje tačno za prirodan broj k. Po pretpostavci polinom $F_{k-1}(x)$ ima realne jednostruke nule x_i, $i = 1,2,\ldots k-2$, koje se nalaze u intervalu $(0,1)$. No, tada funkcija $(x^2-x)F_{k-1}(x)$ zadovoljava u svim intervalima $[x_{i-1},x_i]$, $i = 1,2,\ldots k-1$, $x_o=0$, $x_{k-1}=1$, uslove Roll-ove teoreme, pa u svakom od intervala (x_{i-1},x_i) postoji bar jedna vrednost c_i, $i = 1,2,\ldots,k-1$ takva da je

$$[(x^2 - x)F_{k-1}(x)]'_{x=c_i} = 0.$$

Na osnovu (3.39) sledi

$$F_k(c_i) = 0, \quad i=1,2,\ldots,k-1.$$

Kako je polinom $F_k(x)$ $(k-1)$-og stepena, to su $x=c_i$ sve njegove nule. Time je iz pretpostavke da je tvrdjenje tačno za neko $k-1$, $k\geq 3$, dokazano da je tvrdjenje tačno za prirodan broj k, pa kako je tvrdjenje bilo tačno i za $k=2$, to prema principu matematičke indukcije zaključujemo da je tvrdjenje tačno za svako $k\geq 2$.

Dokaz leme je sad vrlo jednostavan. Jasno je da ako su c_i, $0<c_i<1$, $i=1,2,\ldots,k-1$, koreni polinoma $F_k(x)$, da su $x_i = \frac{1}{c_i} > 1$, $i=1,2,\ldots,k-1$, koreni polinoma $D_k(x)$. S druge strane, prema lemi 3.9, ako je x_i koren polinoma $D_k(x)$, tada je $x_i(x_i - 1)^{-1}$ takodje koren polinoma $D_k(x)$, pa raspodela korena na intervale

$(1,2)$ i $(2,+\infty)$ sledi na osnovu toga što je

$$1<x<2 \Leftrightarrow \frac{x}{x-1} > 2, \quad x>2 \Leftrightarrow 1 < \frac{x}{x-1} < 2.$$

Time je lema u potpunosti dokazana.

Mi smo u lemama 3.3 i 3.7 izveli dve rekurentne formule koje zadovoljava niz $D_k(x)$. Izvedimo sad za niz $D_k(x)$ još jednu rekurentnu formulu.

Lema 3.13 Neka je p proizvoljan neparan broj i neka je

$$s_n = 1^n + 3^n + \ldots + p^n + (-1)^n(2^n + 4^n + \ldots + (p-1)^n), \quad 1 \leqslant n \leqslant k.$$

Neka je dalje

$$\alpha_n = \begin{cases} xs_n, & n \text{ parno} \\ (2-x)s_n, & n \text{ neparno} \end{cases}.$$

Tada je

$$[(p+1)x-1]D_k(x) = s_k x^{k+1} - [D(x)-\alpha x]^k, \tag{3.40}$$

gde je $D^m(x) = D_m(x)$, $\alpha^m = \alpha_m$, $m=1,2,\ldots,k$.

Dokaz. U dokazu leme 3.7 dokazali smo da važi (3.30). Stavljajući u (3.30) redom $m=0,-1,2,-3,4,\ldots,p-1,-p$ i sabirajući sve dobijene determinante, dobijamo determinantu u čijoj se n-toj vrsti, prvoj koloni, $1 \leqslant n \leqslant k-1$, nalazi element

$$1 + (-1)^n(x-1) + [(1+2)^n + 2^n(x-1)] + [(1-3)^n + (-3)^n(x-1)] + \ldots + [(1+(p-1))^n + (p-1)^n(x-1)] + [(1-p)^n + (-p)^n(x-1)] = 1^n + 3^n + \ldots + p^n + (-1)^n(2^n + 4^n + \ldots + (p-1)^n) + (1^n + 3^n + \ldots + p^n + (-1)^n(2^n + 4^n + \ldots + (p-1)^n))(x-1) + (-1)^n(1^n + 3^n + \ldots + p^n)(x-1) = [1^n + 3^n + \ldots + p^n + (-1)^n(2^n + 4^n + \ldots + (p-1)^n)][1 + (-1)^n(x-1)] = s_n[1 + (-1)^n(x-1)] = \alpha_n.$$

U k-toj vrsti, prvoj koloni, nalazi se element

$$\alpha_k - x[(-1)^k + 2^k + (-3)^k + \ldots + (p-1)^k + (-p)^k] = \alpha_k + (-1)^{k-1}xs_k.$$

Drugim rečima, sabiranjem $(p+1)$-ne iste determinante $D_k(x)$, dobijamo

$$(p+1)D_k(x) = \begin{vmatrix} \alpha_1 & x & 0 & \dots & 0 \\ \alpha_2 & \binom{2}{1} & x & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ \alpha_{k-1} & \binom{k-1}{1} & \binom{k-1}{2} & \dots & x \\ \alpha_k + (-1)^{k-1} x s_k & \binom{k}{1} & \binom{k}{2} & \dots & \binom{k}{k-1} \end{vmatrix} . \qquad (3.41)$$

Rastavljajući determinantu (3.41) na dve i razlažući prvu od njih po elementima prve kolone, dobijamo

$$(p+1)D_k(x) = \begin{vmatrix} \alpha_1 & x & 0 & \dots & 0 \\ \alpha_2 & \binom{2}{1} & x & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ \alpha_{k-1} & \binom{k-1}{1} & \binom{k-1}{2} & \dots & x \\ \alpha_k & \binom{k}{1} & \binom{k}{2} & \dots & \binom{k}{k-1} \end{vmatrix} +$$

$$+ \begin{vmatrix} 0 & x & 0 & \dots & 0 \\ 0 & \binom{2}{1} & x & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & \binom{k-1}{1} & \binom{k-1}{2} & \dots & x \\ (-1)^{k-1} x s_k & \binom{k}{1} & \binom{k}{2} & \dots & \binom{k}{k-1} \end{vmatrix} = \alpha_1 A_{1,k}(x) -$$

$$- \alpha_2 x A_{2,k}(x) + \dots + (-1)^{k-2} \alpha_{k-1} x^{k-2} A_{k-1,k}(x) +$$

$$+ (-1)^{k-1} \alpha_k x^{k-1} + s_k x^k = \binom{k}{1} \alpha_1 D_{k-1}(x) - \binom{k}{2} \alpha_2 x D_{k-2}(x) +$$

$$+ \dots + \binom{k}{k-1} (-1)^{k-2} \alpha_{k-1} x^{k-2} D_1(x) + (-1)^{k-1} \alpha_k x^{k-1} + s_k x^k .$$

Množeći dobijenu jednakost sa $(-x)$ i dodavajući obema stranama $D_k(x)$, dobijamo (3.40), što je i trebalo dokazati.

Napomenimo na kraju našeg razmatranja niza $D_k(x)$, da se niz polinoma $D_k(x)$ može dovesti u vezu sa jednim drugim nizom polinoma $P_k(x)$ definisanim sa

$$P_k(x) = \left[\frac{d^k \ln(a+bx^v)}{dv^k}\right]_{v=0}, \quad x = \frac{b}{a}. \tag{3.41}$$

Naime, može da se pokaže da važi jednakost

$$P'_k(x) = (-1)^k x^{k-1} D_k\left(\frac{1}{x}\right), \quad x \neq 0. \tag{3.42}$$

Niz $P_k(x)$ pominju u svojim radovima Hilbert* i Saalschütz**, a primenjuju na Fermat-ov problem Krasner [22] i Brückner [5]. Primetimo ovde, da se definicija niza $D_k(x)$ pokazala mnogo elastičnijom od definicije niza $P_k(x)$, što proističe iz činjenice da smo niz $D_k(x)$ ispitali više, nego što je to, tokom vremena, učinjeno sa nizom $P_k(x)$. (Na primer, pitanje racionalnosti nula.) Posledica ovoga je da se niz $D_k(x)$ pokazao uspešnijim od niza $P_k(x)$ u primeni na Fermat-ov problem, u što ćemo uskoro da se uverimo.

*Jahresb. die Deut. Mat. Ver. IV (1894-1895), 175.

**Journ. für die reine und ang. Math. 123 (1901), 210.

IV G L A V A

4.1 Osnovna teorema

Sada smo u mogućnosti da, kao što smo obećali u odeljku 1.7, dokažemo teoremu ekvivalentnu teoremi 1.14. Kao što ćemo uskoro videti, glavnu ulogu će tu da igra niz polinoma $D_k(x)$, kojeg smo definisali i čije osobine smo ispitali u prethodnoj glavi.

Teorema 4.1 Da bi jednačina

$$x^p + y^p = z^p, \quad x,y,z \in N, \quad p \in P, \quad p \geq 3 \tag{4.1}$$

imala rešenja relativno prosta sa p, potrebno je da postoji t, takvo da sve tri vrednosti

$$t, \ \frac{1}{t}, \ 1-t \tag{4.2}$$

zadovoljavaju svih $\frac{p-1}{2}$ kongruencija

$$B_{p-k-1} D_k(t) \equiv 0 \pmod p, \quad k=2,4,6,\ldots p-3,p-2, \tag{4.3}$$

gde su B_{p-k-1} Bernoulli-jevi brojevi, a $D_k(t)$ polinomi odredjeni sa (3.11).

Dokaz. Očigledno važi

$$(1-ve^u) \sum_{m=o}^{p-1} (ve^u)^m = 1 - v^p e^{pu},$$

odnosno,

$$(1-ve^u) \sum_{m=1}^{p-1} (ve^u)^m = ve^u - v^p e^{pu}. \tag{4.4}$$

Diferencirajući k puta jednakost (4.4) po u, primenom Leibnitzove formule dobijamo

$$ve^u - p^k v^p e^{pu} = -ve^u \left[\binom{k}{o} \sum_{m=1}^{p-1} (ve^u)^m + \binom{k}{1} \sum_{m=1}^{p-1} m(ve^u)^m + \right.$$

$$+ \binom{k}{2} \sum_{m=1}^{p-1} m^2 (ve^u)^m + \ldots + \binom{k}{k-1} \sum_{m=1}^{p-1} m^{k-1} (ve^u)^m] +$$

$$+ (1-ve^u) \sum_{m=1}^{p-1} m^k (ve^u)^m. \qquad (4.5)$$

Za $u=o$, (4.5) postaje

$$v - p^k v^p = -v [\binom{k}{o} \sum_{m=1}^{p-1} v^m + \binom{k}{1} \sum_{m=1}^{p-1} m v^m + \binom{k}{2} \sum_{m=1}^{p-1} m^2 v^m +$$

$$+ \ldots + \binom{k}{k-1} \sum_{m=1}^{p-1} m^{k-1} v^m] + (1-v) \sum_{m=1}^{p-1} m^k v^m. =$$

$$= - v \sum_{m=o}^{k-1} \binom{k}{m} f_{m+1}(v) + (1-v) f_{k+1}(v),$$

gde je

$$f_k(v) = \sum_{m=1}^{p-1} m^{k-1} v^m, \quad k \in N.$$

Nakon sredjivanja, za $v \neq o$ izlazi

$$p^k v^{p-1} - 1 = \sum_{m=o}^{k-1} \binom{k}{m} f_{m+1}(v) + \frac{v-1}{v} f_{k+1}(v), \quad k \in N. \qquad (4.6)$$

S druge strane, stavljajući u (4.4) $u=o$, izlazi

$$v^{p-1} - 1 = \frac{v-1}{v} f_1(v). \qquad (4.7)$$

Neka je $v \neq 0$, $v \neq 1$ i neka je $t = \frac{v-1}{v}$, $t \neq 0$. Na osnovu (4.6) i (4.7) raspolažemo sledećim sistemom jednačina.

$$\begin{aligned}
& t f_1(v) = v^{p-1} - 1, \\
& f_1(v) + t f_2(v) = p v^{p-1} - 1, \\
& f_1(v) + \binom{2}{1} f_2(v) + t f_3(v) = p^2 v^{p-1} - 1, \\
& f_1(v) + \binom{3}{1} f_2(v) + \binom{3}{2} f_3(v) + t f_4(v) = p^3 v^{p-1} - 1, \\
& \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
& f_1(v) + \binom{k}{1} f_2(v) + \ldots + \binom{k}{k-1} f_k(v) + t f_{k+1}(v) = p^k v^{p-1} - 1.
\end{aligned} \qquad (4.8)$$

Neka je $C(t)$ determinanta sistema (4.8). Očigledno je

$$C(t) = t^{k+1} = (\frac{v-1}{v}.)^{k+1} \neq 0. \tag{4.9}$$

Iz (4.8) i (4.9) sledi

$$t^{k+1} f_{k+1}(v) = C_{k+1}(v), \tag{4.10}$$

gde je $C_{k+1}(v)$ determinanta

$$C_{k+1}(v) = \begin{vmatrix} t & 0 & 0 & 0 & \dots & 0 & v^{p-1} - 1 \\ 1 & t & 0 & 0 & \dots & 0 & pv^{p-1} - 1 \\ 1 & \binom{2}{1} & t & 0 & \dots & 0 & p^2 v^{p-1} - 1 \\ 1 & \binom{3}{1} & \binom{3}{2} & t & \dots & 0 & p^3 v^{p-1} - 1 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 1 & \binom{k}{1} & \binom{k}{2} & \binom{k}{3} & \dots & \binom{k}{k-1} & p^k v^{p-1} - 1 \end{vmatrix}.$$

Razbijajući determinantu $C_{k+1}(v)$ na zbir dve determinante, dobijamo

$$C_{k+1}(v) = \begin{vmatrix} t & 0 & 0 & 0 & \dots & 0 & v^{p-1} - 1 \\ 1 & t & 0 & 0 & \dots & 0 & pv^{p-1} \\ 1 & \binom{2}{1} & t & 0 & \dots & 0 & p^2 v^{p-1} \\ 1 & \binom{3}{1} & \binom{3}{2} & t & \dots & 0 & p^3 v^{p-1} \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 1 & \binom{k}{1} & \binom{k}{2} & \binom{k}{3} & \dots & \binom{k}{k-1} & p^k v^{p-1} \end{vmatrix} +$$

$$+ \begin{vmatrix} t & 0 & 0 & 0 & \dots & 0 & 0 \\ 1 & t & 0 & 0 & \dots & 0 & -1 \\ 1 & \binom{2}{1} & t & 0 & \dots & 0 & -1 \\ 1 & \binom{3}{1} & \binom{3}{2} & t & \dots & 0 & -1 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 1 & \binom{k}{1} & \binom{k}{2} & \binom{k}{3} & \dots & \binom{k}{k-1} & -1 \end{vmatrix}. \tag{4.11}$$

Neka je $v \not\equiv 0 \pmod p$. Tada je $v^{p-1} - 1 \equiv 0 \pmod p$, pa su u prvoj determinanti u jednakosti (4.11) svi elementi poslednje kolone deljivi sa p. Sledi

$$C_{k+1}(v) \equiv t \begin{vmatrix} t & 0 & 0 & \dots & 0 & -1 \\ \binom{2}{1} & t & 0 & \dots & 0 & -1 \\ \binom{3}{1} & \binom{3}{2} & t & \dots & 0 & -1 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ \binom{k}{1} & \binom{k}{2} & \binom{k}{3} & \dots & \binom{k}{k-1} & -1 \end{vmatrix} =$$

$$= (-1)^k t \begin{vmatrix} 1 & t & 0 & 0 & \dots & 0 \\ 1 & \binom{2}{1} & t & 0 & \dots & 0 \\ 1 & \binom{3}{1} & \binom{3}{2} & t & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 1 & \binom{k}{1} & \binom{k}{2} & \binom{k}{3} & \dots & \binom{k}{k-1} \end{vmatrix} =$$

$$= (-1)^k t D_k(t) \pmod p. \qquad (4.12)$$

Uzimajući u obzir (4.10) i (4.12), kao i sve učinjene pretpostavke, dobijamo

$$f_{k+1}(v) \equiv (-t)^{-k} D_k(t), \quad v \not\equiv 0, \quad t \not\equiv 0 \pmod p. \qquad (4.13)$$

Prema teoremi 1.14 svih šest vrednosti

$$\frac{x}{z}, \frac{z}{x}, \frac{y}{z}, \frac{z}{y}, -\frac{x}{y}, -\frac{y}{x}$$

mora da zadovoljava svih $\frac{p-1}{2}$ kongruencija

$$B_{p-k} f_k(v) \equiv 0 \pmod p, \quad k=3,5,7,\dots,p-2,p-1. \qquad (4.14)$$

Neka je $z \equiv vx \pmod p$. Očigledno je $v \not\equiv 0$, $v \not\equiv 1 \pmod p$, jer bi u protivnom bilo $z \equiv 0$, odnosno, $y \equiv 0 \pmod p$, što protivreči pretpostavci $xyz \not\equiv 0 \pmod p$. Imajući na umu da je $x + y \equiv z \pmod p$, dobijamo

$$\frac{z}{x} \equiv v, \quad \frac{x}{z} \equiv \frac{1}{v}, \quad \frac{y}{z} \equiv 1 - \frac{1}{v}, \quad \frac{z}{y} \equiv \frac{v}{v-1}, \quad -\frac{x}{y} \equiv \frac{1}{1-v},$$

$$-\frac{y}{x} \equiv 1 - v \pmod p.$$

Neka je $\frac{v-1}{v} = t$. Očigledno je $t \not\equiv 0,\ t \not\equiv 1 \pmod p$. Izlazi

$$v = \frac{1}{1-t},\ \frac{1}{v} = 1-t,\ 1 - \frac{1}{v} = t,\ \frac{v}{v-1} = \frac{1}{t},\ \frac{1}{1-v} = 1 - \frac{1}{t},$$

$$1 - v = \frac{t}{t-1}.$$

Dakle, da bi jednačina (4.1) imala rešenja relativno prosta sa p, potrebno je da svih šest vrednosti

$$t,\ 1-t,\ \frac{1}{t},\ \frac{1}{1-t},\ \frac{t}{t-1},\ 1 - \frac{1}{t} \qquad (4.15)$$

zadovoljava svih $\frac{p-1}{2}$ kongruencija (4.14). Na osnovu (4.13), uzimajući u obzir $v \not\equiv 0,\ t \not\equiv 0 \pmod p$, izlazi da svih šest vrednosti (4.15) moraju da zadovoljavaju svih $\frac{p-1}{2}$ kongruencija (4.3).

Preostalo je da se dokaže da se od brojeva (4.15) mogu u gornjem uslovu zadržati samo prva tri. Prema lemi 3.9 važi

$$D_k(t) = (1-t)^{k-1} D_k\left(\frac{t}{t-1}\right), \quad t \neq 1,$$

$$D_k(1-t) = t^{k-1} D_k\left(1 - \frac{1}{t}\right), \quad t \neq 0,$$

$$D_k\left(\frac{1}{t}\right) = \left(1 - \frac{1}{t}\right)^{k-1} D_k\left(\frac{1}{1-t}\right), \quad t \neq 1,\ t \neq 0.$$

Dakle, ako $t,\ 1-t,\ \frac{1}{t}$ zadovoljavaju svih $\frac{p-1}{2}$ kongruencija (4.3), onda će sve te kongruencije zadovoljavati i $\frac{t}{t-1},\ 1 - \frac{1}{t},\ \frac{1}{1-t}$. Time je teorema u potpunosti dokazana.

4.2 Uslov $B_{p-k-1} \not\equiv 0 \pmod p$

U odeljku 1.7 naveli smo rezultate Cauchy-ja, Kummer-a, Mirimanoff-a i Krasner-a vezane za prvi slučaj Fermat-ovog problema. Sada smo u mogućnosti da, koristeći teoremu 4.1, kao i osobine niza polinoma $D_k(x)$, te rezultate poboljšamo. Pre svega, dokažimo sledeću lemu.

Lema 4.1 Neka je $D_k(t)=(2-t)P_k(t)$, $k=2,4,\ldots,p-3$, $p \in P$, $p>3$ i neka je $Q(t) = t^6 - 3t^5 + \lambda t^4 - (2\lambda-5)t^3 + \lambda t^2 - 3t + 1$. Da bi $t,\ 1-t,\ \frac{1}{t}$ istovremeno zadovoljavali kongruenciju

$$D_k(t) \equiv 0 \pmod p,\ k=2,4,\ldots,p-3, \qquad (4.16)$$

potrebno je da bude ispunjen jedan i samo jedan od sledeća tri uslova:

1° $P_k(-1) \equiv 0 \pmod p$.

2° $P_k(t) \equiv 0 \pmod p \wedge t^2 - t + 1 \equiv 0 \pmod p$.

3° $t^3 + 1 \not\equiv 0 \pmod p$, $k \geq 8$ i svi koeficijenti ostatka deljenja polinoma $P_k(t)$ sa $Q(t)$ su deljivi sa p.

Dokaz. Neka su vrednosti

$$t,\ 1-t,\ \frac{1}{t} \tag{4.17}$$

istovremeno rešenje kongruencije (4.16). Vrednosti (4.17) su medjusobno kongruentne po modulu p jedino ako je ispunjena jedna od kongruencija

$$t^2 \equiv 1,\ 2t \equiv 1,\ t^2 - t + 1 \equiv 0 \pmod p.$$

Sledi

$$t \equiv 1,\ t \equiv -1,\ t \equiv \frac{1}{2},\ t^2 - t + 1 \equiv 0 \pmod p.$$

Prema lemama 3.8 i 3.9 je

$$D_k(1) = 1,\ D_k(\tfrac{1}{2}) = (1 - \tfrac{1}{2})^{k-1} D_k(-1),$$

pa mogućnost $t \equiv 1 \pmod p$ otpada, a mogućnost $t \equiv \frac{1}{2} \pmod p$ se svodi na $t \equiv -1 \pmod p$.

Znači, u slučaju da su vrednosti (4.17) medjusobno kongruentne po modulu p mora biti ispunjena jedna i samo jedna (zbog $p>3$) kongruencija

$$t \equiv -1 \pmod p,\ t^2 - t + 1 \equiv 0 \pmod p.$$

U protivnom, biće

$$t^3 + 1 \not\equiv 0 \pmod p.$$

Razmotrimo redom sva tri slučaja.

1° Za $t \equiv -1 \pmod p$, mora biti $D_k(-1) \equiv 0 \pmod p$. Kako je k parno, to je, na osnovu leme 3.10, $D_k(t) = (2-t)P_k(t)$, pa sledi

$$P_k(-1) \equiv 0 \pmod p.$$

2° Za $t^2 - t + 1 \equiv 0 \pmod p$ je $t \not\equiv 2 \pmod p$ (jer je $p>3$). No, onda iz $D_k(t) \equiv 0 \pmod p$ sledi

$$P_k(t) \equiv 0 \pmod p.$$

3° Neka je $t^3 + 1 \not\equiv 0 \pmod p$. Tada su, ne samo vrednosti (4.17), nego i vrednosti (4.15) medjusobno inkongruentne po modulu p.

Jasno je da ako vrednosti (4.17) zadovoljavaju kongruenciju (4.16), da tu kongruenciju onda zadovoljavaju i vrednosti (4.15). Dakle, kongruenciju (4.16) zadovoljavaju šest, medjusobno nekongruentnih vrednosti (4.15).

Kako je

$$D_k(t) = (2-t)P_k(t),$$

to iz

$$D_k(t) \equiv 0 \pmod p \Rightarrow P_k(t) \equiv 0 \pmod p.$$

Stvarno, ako bi bilo $t \equiv 2 \pmod p$, sledilo bi $1-t \equiv -1 \pmod p$, tj. $D_k(-1) \equiv 0 \pmod p$, što je nemoguće zbog uslova $t^3 + 1 \not\equiv 0 \pmod p$.

Polinom $P_k(t)$ je $(k-2)$-og stepena, a kongruencija

$$P_k(t) \equiv 0 \pmod p \qquad (4.18)$$

ima šest nekongruentnih rešenja. Sledi, $k-2 \geq 6$, tj. $k \geq 8$. Stvarno, za $k-2<6$, kongruencija (4.18) bi imala veći broj nekongruentnih rešenja od stepena polinoma $P_k(t)$, pa bi, na osnovu poznatog stava, svi koeficijenti polinoma $P_k(t)$ morali biti deljivi sa p. To je, medjutim, nemoguće, jer je, izmedju ostalog, najstariji koeficijent polinoma $P_k(t)$ jednak 1 (najstariji koeficijent polinoma $D_k(t)$ je $(-1)^{k-1} = -1$).

S druge strane, ako su

$$a, \frac{1}{a}, 1-a, 1-\frac{1}{a}, \frac{a}{a-1}, \frac{1}{1-a}, \quad a \neq 0, \quad a \neq 1,$$

koreni polinoma šestog stepena, tada se taj polinom može napisati u obliku

$$Q(t) = t^6 - 3t^5 + \lambda t^4 - (2\lambda-5)t^3 + \lambda t^2 - 3t + 1,$$

gde je

$$\lambda = 6 - \frac{(a^2 - a + 1)^3}{(a^2 - a)^2}.$$

Neka je

$$P_k(t) = Q(t)F_k(t) + R_k(t). \qquad (4.19)$$

S obzirom na način na koji je odredjen polinom $Q(t)$, jasno da ako za neko t važi $Q(t) \equiv 0 \pmod p$, da će tada kongruencija

$$Q(t) \equiv 0 \pmod p$$

biti zadovoljena za svih šest vrednosti (4.15). Kako kongruencija (4.18) ima šest nekongruentnih rešenja (4.15), to na osnovu (4.19) sledi da kongruencija

$$R_k(t) \equiv 0 \pmod p$$

ima šest nekongruentnih rešenja (4.15). Polinom $R_k(t)$ je najviše petog stepena, pa svi njegovi koeficijenti moraju biti deljivi sa p.

Time je lema u potpunosti dokazana.

Primetimo ovde, da koeficijenti ostatka $R_k(t)$ zavise od λ, pa se u slučaju 3^o dobija kao uslov da moraju biti zadovoljene šest kongruencija $(mod\ p)$ po λ. Tih šest kongruencija se, u stvari, svode na tri, pošto će dve po dve da budu saglasne (zbog toga što ako su vrednosti(4.17) rešenja kongruencije $D_k(t) \equiv 0\ (mod\ p)$, tada su i $\frac{t}{t-1}$, $1 - \frac{1}{t}$, $\frac{1}{1-t}$ takodje rešenja te kongruencije).Eliminisanjem λ iz tih kongruencija dobija se

$$N_1 \equiv 0 \pmod p, \quad N_2 \equiv 0 \pmod p,$$

odnosno, konačno

$$(N_1, N_2) \equiv 0 \pmod p.$$

Sada se dokaz teoreme, koja predstavlja poboljšanje uslova (1.67)-(1.69), svodi, kao što ćemo videti, na običan račun.

Teorema 4.2 Ako je bar za jedno k, $k=2,4,6,8,10,12$, ispunjeno

$$B_{p-k-1} \not\equiv 0 \pmod p, \tag{4.20}$$

tada jednačina (4.1) nema rešenja relativno prosta sa p, $p \neq 3,5,7,11,13,19,41,43,223,2731,36389,75571,20579903$.

Dokaz. Prema teoremi 4.1, tvrdjenje će biti dokazano, ako dokažemo da t, $1-t$, $\frac{1}{t}$ ne mogu istovremeno biti rešenja kongruencije

$$D_k(t) \equiv 0 \pmod p \tag{4.21}$$

za svako $k=2,4,\ldots,12$. Imajući na umu lemu 4.1, uvodeći oznake

$$P_k(t) = t^{k-2} + b_{k-3}t^{k-3} + \ldots + b_1 t + b_o,$$

$$F_k(t) = t^{k-8} + c_{k-9}t^{k-9} + \ldots + c_1 t + c_o,$$

$$R_k(t) = d_5 t^5 + d_4 t^4 + d_3 t^3 + d_2 t^2 + d_1 t + d_o,$$

gde je

$$D_k(t) = (2-t)P_k(t), \quad P_k(t) = Q(t)F_k(t) + R_k(t),$$

$$Q(t) = t^6 - 3t^5 + \lambda t^4 - (2\lambda-5)t^3 + \lambda t^2 - 3t + 1$$

i izračunavajući koeficijente $a_{n,k}$ polinoma $D_k(t)$ bilo na osnovu leme 3.5, odnosno (3.16), bilo na osnovu teoreme 3.3, odnosno (3.19)-(3.26), dobijamo redom.

1° $k=2$. $D_2(t)=2-t$, $P_2(t)=1$. Dolazi u obzir samo $D_2(-1) \equiv 0 \pmod p$, odnosno, $p=3$.

2° $k=4$. $D_4(t) = -t^3 + 14t^2 - 36t + 24$,

$P_4(t) = t^2 - 12t + 12$.

a) $t \equiv -1 \pmod p \Rightarrow p \mid 3\cdot 5^2 \Rightarrow p=3,5$.

b) $t^2 - t + 1 \equiv 0 \pmod p \wedge P_4(t) \equiv 0 \pmod p \Rightarrow 11t^2 \equiv 0 \pmod p \Rightarrow p = 11$, što je nemoguće, jer je $11=6\cdot 1+5$, a svi prosti faktori broja $t^2 - t + 1$ moraju biti oblika $6m + 1$.

3° $k=6$. $D_6(t) = -t^5 + 62t^4 - 540t^3 + 1560t^2 - 1800t + 720$,

$P_6(t) = t^4 - 60t^3 + 420t^2 - 720t + 360$.

a) $t \equiv -1 \pmod p \Rightarrow p \mid 3\cdot 7\cdot 223 \Rightarrow p=3,7,223$.

b) $t^2 - t + 1 \equiv 0 \pmod p \wedge P_6(t) \equiv 0 \pmod p \Rightarrow 420t^2 - 721t + 420 \equiv 0 \pmod p \Rightarrow p \mid 7\cdot 43 \Rightarrow p=7,43$.

4° $k=8$. $D_8(t) = -t^7 + 254t^6 - 5796t^5 + 40824t^4 - 126000t^3 + 191520t^2 - 141120t + 40320$,

$P_8(t) = t^6 - 252t^5 + 5292t^4 - 30240t^3 + 65520t^2 - 60480t + 20160$.

a) $t \equiv -1 \pmod p \Rightarrow p \mid 3\cdot 5\cdot 36389 \Rightarrow p=3,5,36389$.

b) $t^2 - t + 1 \equiv 0 \pmod p \wedge P_8(t) \equiv 0 \pmod p \Rightarrow 65772t^2 - 65772t + 50401 \equiv 0 \pmod p \Rightarrow p \mid 19\cdot 809 \Rightarrow p=19$, pošto je $809 \equiv 5 \pmod 6$.

c) $F_8(t) = 1$,

$R_8(t) = -249t^5 + (5292-\lambda)t^4 + (2\lambda-30245)t^3 + (65520-\lambda)t^2 -$

$- 60477t + 20143.$

Kako je $(343, 20159)=1$, to izlazi $p=1$, što je nemoguće.

5° $k=10$. $D_{10}(t) = - t^9 + 1022t^8 - 55980t^7 + 818320t^6 - 5103600t^5 +$

$+ 16435440t^4 - 29635200t^3 + 30240000t^2 - 16329600t +$

$+ 3628800,$

$P_{10}(t) = t^8 - 1020t^7 + 53940t^6 - 710640t^5 + 3681720t^4 -$

$- 9072000t^3 + 11491200t^2 - 7257600t + 1814400.$

a) $t \equiv -1 \pmod p \Rightarrow p \mid 3 \cdot 11 \cdot 41 \cdot 75571 \Rightarrow p=3, 11, 41, 75571.$

b) $t^2 - t + 1 \equiv 0 \pmod p \wedge P_{10}(t) \equiv 0 \pmod p. \Rightarrow 12201841t^2 -$

$- 10940340t + 10940340 \equiv 0 \pmod p \Rightarrow p \mid 683 \cdot 1847$, što je nemoguće, jer je $683 \equiv 1847 \equiv 5 \pmod 6$.

c) $F_{10}(t) = t^2 + c_1 t + c_o$. Mora biti

$c_1 - 3 = b_7,$

$c_o - 3c_1 + \lambda = b_6,$

$d_5 = b_5 + 3c_o - \lambda c_1 + 2\lambda - 5,$

$d_4 = b_4 - \lambda c_o + (2\lambda-5)c_1 - \lambda,$

$d_3 = b_3 + (2\lambda-5)c_o - \lambda c_1 + 3,$

$d_2 = b_2 - \lambda c_o + 3c_1 - 1,$

$d_1 = b_1 + 3c_o - c_1,$

$d_o = b_o - c_o.$

Eliminisanjem c_o i c_1 nalazimo

$d_o = \lambda + (b_o - b_6 - 3b_7 - 9),$

$d_1 = - 3\lambda + (b_1 + 3b_6 + 8b_7 + 24),$

$d_2 = \lambda^2 - (b_6 + 3b_7 + 9)\lambda + (b_2 + 3b_7 + 8),$

$d_3 = - 2\lambda^2 + (2b_6 + 5b_7 + 20)\lambda - (-b_3 + 5b_6 + 15b_7 + 42),$

$d_4 = \lambda^2 - (b_6 + b_7 + 4)\lambda + (b_4 - 5b_7 - 15),$

$d_5 = - (b_7 + 4)\lambda + (b_5 + 3b_6 + 9b_7 + 22).$

Eliminišući λ iz kongruencija $d_i \equiv 0 \pmod p$, $i=0,1,\ldots 5$, dobijamo

$N_1 = 1012383 \equiv 0 \pmod p$, $N_2 = 903196621 \equiv 0 \pmod p$.

Kako je, što nije teško utvrditi Euklid-ovim algoritmom, $(N_1, N_2) = 1$, to sledi $p = 1$, što je nemoguće.

6° $k=12$. $D_{12}(t) = -t^{11} + 4094t^{10} - 519156t^9 + 14670024t^8 -$
$- 165528000t^7 + 953029440t^6 - 3162075840t^5 + 6411968640t^4 -$
$- 8083152000t^3 + 6187104000t^2 + 2634508800t + 479001600,$
$P_{12}(t) = t^{10} - 4092t^9 + 510972t^8 - 13654080t^7 + 138219840t^6 -$
$- 676589760t^5 + 1808896320t^4 - 2794176000t^3 + 2494800000t^2 -$
$- 1197504000t + 239500800.$

a) $t \equiv -1 \pmod p \Rightarrow p \mid 3 \cdot 5 \cdot 7 \cdot 13 \cdot 20579903 \Rightarrow p = 3, 5, 7, 13, 20579903.$

b) $t^2 - t + 1 \equiv 0 \pmod p \wedge P_{12}(t) \equiv 0 \pmod p \Rightarrow 3171900732t^2 -$
$- 3020054401t + 3171900732 \equiv 0 \pmod p \Rightarrow p \mid 7 \cdot 13^2 47 \cdot 2731$
$\Rightarrow p = 7, 13, 2731,$ pošto je $47 \equiv 5 \pmod 6$.

c) $F_{12}(t) = t^4 + c_3 t^3 + c_2 t^2 + c_1 t + c_o$. Mora biti

$c_3 - 3 = b_9,$
$c_2 - 3c_3 + \lambda = b_8,$
$c_1 - 3c_2 + \lambda c_3 - (2\lambda - 5) = b_7,$
$c_o - 3c_1 + \lambda c_2 - (2\lambda - 5)c_3 + \lambda = b_6,$
$d_5 = b_5 + 3c_o - \lambda c_1 + (2\lambda - 5)c_2 - \lambda c_3 + 3,$
$d_4 = b_4 - \lambda c_o + (2\lambda - 5)c_1 - \lambda c_2 + 3c_3 - 1,$
$d_3 = b_3 + (2\lambda - 5)c_o - \lambda c_1 + 3c_2 - c_3,$
$d_2 = b_2 - \lambda c_o + 3c_1 - c_2,$
$d_1 = b_1 + 3c_o - c_1,$
$d_o = b_o - c_o.$

Eliminišući c_o, c_1, c_2, c_3, nakon sredjivanja izlazi iz $d_i \equiv 0 \pmod p$, $i = 0, 1, \ldots 5$.

$(b_9+5)\lambda^2 - (b_7+4b_8+16b_9+50)\lambda + (b_5+3b_6+9b_7+22b_8+51b_9+$
$+111) \equiv 0 \pmod p,$

$$\lambda^3 - (b_8+2b_9+3)\lambda^2 + (b_6+b_7+4b_8+2b_9-4)\lambda + (-b_4+5b_7+15b_8+$$
$$+42b_9+102) \equiv 0 \pmod p,$$
$$-2\lambda^3 + (2b_8+7b_9+33)\lambda^2 - (2b_6+5b_7+20b_8+55b_9+157)\lambda +$$
$$+ (-b_3+5b_6+15b_7+42b_8+102b_9+231) \equiv 0 \pmod p,$$
$$\lambda^3 - (b_8+4b_9+16)\lambda^2 + (b_6+3b_7+9b_8+25b_9+62)\lambda - (b_2+3b_7+$$
$$+8b_8+24b_9+57) \equiv 0 \pmod p,$$
$$-3\lambda^2 + (3b_8+11b_9+44)\lambda - (b_1+3b_6+8b_7+24b_8+57b_9+131) \equiv 0$$
$$\pmod p,$$
$$\lambda^2 - (b_8+4b_9+16)\lambda + (-b_o+b_6+3b_7+9b_8+22b_9+51) \equiv 0 \pmod p.$$

Eliminišući λ iz ovih kongruencija nalazimo da mora biti $N_1 = 488295218281 \equiv 0 \pmod p$, $N_2 = 57242173091237511 \equiv 0 \pmod p$. Primenjujući Euklid-ov algoritam nalazimo $(N_1, N_2)=13$, pa mora biti $p=13$.

Rezimirajući dobijene rezultate uvidjamo da t, $1-t$, $\frac{1}{t}$ mogu biti istovremeno rešenja kongruencije $D_k(t) \equiv 0 \pmod p$ jedino za:

k	p
2	3
4	3, 5
6	3, 7, 43, 223
8	3, 5, 19, 36389
10	3, 11, 41, 75571
12	3, 5, 7, 13, 2731, 20579903

Sa ovim je teorema u potpunosti dokazana.

Primetimo ovde, da izuzete vrednosti p i nisu naročito interesantne. Naime, brojevi 3, 5, 7, 11, 13, 19, 41, 43, 223, 2731 su regularni, pa za njih jednačina (4.1) i onako nema rešenja. Za preostala tri prosta broja 36389, 75571, 20579903, ukoliko nisu regularni, može se primeniti teorema 4.2, izuzimajući $k=8,10,12$, respektivno.

Primetimo dalje, da se teorema 4.2 očigledno može proširiti, diskutujući istom metodom kongruencije $D_k(t) \equiv 0 \pmod p$, za $k=14,16,\ldots 2N$. Naravno, račun postaje sve duži i mukotrpniji

i zahteva obaveznu primenu računara, koji za $k<12$ nije korišćen.

Teorema 4.2 predstavlja, očigledno, poboljšanje rezultata Cauchy-ja, Kummer-a i Mirimanoff-a iskazanih uslovima (1.67)-(1.69). Ovde bi bilo zanimljivo, uporediti rezultat iskazan teoremom 4.2 sa rezultatom Krasner-a, pomenutim u odeljku 1.7. Podsetimo se, Krasner je pokazao sledeće: Postoji p_o (koji može biti efektivno izračunat) takav da za $p \geq p_o$ jednačina (4.1) može imati rešenja relativno prosta sa p samo pod uslovom da je za svako $k=2,4,\ldots,2k_o$, $k_o=[\sqrt[3]{ln\, p}]$, ispunjeno

$$B_{p-k-1} \equiv 0 \pmod{p}.$$

Jasno je odmah da je za dovoljno veliko p Krasner-oy kriterijum esencijalno strožiji od kriterijuma iskazanim teoremom 4.2. Medjutim, p stvarno mora biti vrlo veliko da bi, zanemarujući uslov $p \geq p_o$, bilo ispunjeno $\sqrt[3]{ln\, p} \geq 7$. Naime, ova nejednakost je ispunjena za $p \geq e^{343} > 9,18 \cdot 10^{148}$. Drugim rečima, tek za $p \geq max(p_o, e^{343})$ Krasner-ov kriterijum je strožiji. Na taj način, i pored Krasner-ovog rezultata (i rezultata tog tipa), opravdano je iskazivanje teoreme 4.2.

Naš će cilj sada da bude da poboljšamo Krasner-ov rezultat, i to u dva pravca. S jedne strane, pokazaćemo da za p nije potrebno uvoditi nikakva ograničenja, a sa druge, da umesto $\sqrt[3]{ln\, p}$ može da stoji $\frac{1}{2}(1+\sqrt[5]{ln^2 p})$. Uz sve to, iskoristićemo i dobre osobine teoreme 4.2. Dokažimo sledeću teoremu.

Teorema 4.3 Ako je bar za jedno k, $k=2,4,\ldots,2k_o$, $k_o = max(6, [\frac{1}{2}(1+\sqrt[5]{ln^2 p})])$, ispunjeno

$$B_{p-k-1} \not\equiv 0 \pmod{p}, \qquad (4.22)$$

tada jednačina (4.1) nema rešenja relativno prosta sa p, $p \neq 3,5,7,11,13,19,41,43,223,2731,36389,75571,20579903$.

Dokaz. Ako je $k_o \leq 6$, teorema je dokazana na osnovu teoreme 4.2. Neka je, dakle, $k_o \geq 7$, tj. $k \geq 14$.

Pretpostavimo suprotno tvrdjenju teoreme: neka za neko k, $k=14,\ldots,2k_o$, $k_o=[\frac{1}{2}(1+\sqrt[5]{ln^2 p})]$, važi (4.22) i neka pri tom jednačina(4.1) ima rešenja relativno prosta sa p. Prema teoremi 4.1 moraju tada t, $\frac{1}{t}$, $1-t$ da zadovoljavaju kongruenciju

$$D_k(t) \equiv 0 \pmod{p}.$$

Ako je R_k rezolventa polinoma $D_k(t)$ i $t^{k-1}D_k(\frac{1}{t})$, tada očigledno mora biti

$$R_k \equiv 0 \pmod{p}. \tag{4.23}$$

Prema lemi 3.12 polinom $D_k(t)$ ima sve nule realne i jednostruke i pri tome su sve nule u intervalu $(1,+\infty)$. Ako su t_i, $i=1,2,\ldots,k-1$, nule polinoma $D_k(t)$, tada su $x_i = \frac{1}{t_i}$ nule polinoma $t^{k-1}D_k(\frac{1}{t})$ i pri tome je, prema lemi 3.12, $0<x_i<1$. Znači, polinomi $D_k(t)$ i $t^{k-1}D_k(\frac{1}{t})$ nemaju zajedničke nule, pa je $R_k \neq 0$.

Kako je

$$\prod_{i=1}^{k-1} t_i = x_{k,k} = k!,$$

to dobijamo

$$0 < |R_k| = (k!)^{k-1} \prod_{1\leqslant i,j\leqslant k-1} (t_i - \frac{1}{t_j}) =$$

$$= (k!)^{2(k-1)} \prod_{1\leqslant i,j\leqslant k-1} (1 - x_i x_j). \tag{4.24}$$

Stavljajući

$$A = \prod_{1\leqslant i,j\leqslant k-1} (1 - x_i x_j),$$

sledi

$$\ln A = \sum_{1\leqslant i,j\leqslant k-1} \ln(1 - x_i x_j) = -\sum_{1\leqslant i,j\leqslant k-1} \sum_{n=1}^{\infty} \frac{(x_i x_j)^n}{n} =$$

$$= -\sum_{n=1}^{\infty} \frac{1}{n}\Big[\sum_{i=1}^{k-1} x_i^n\Big]^2 < -\sum_{n=1}^{5} \frac{1}{n}\Big[\sum_{i=1}^{k-1} x_i^n\Big]^2 =$$

$$= -\sum_{n=1}^{5} \frac{s_n^2}{n}, \tag{4.25}$$

gde je

$$s_n = \sum_{i=1}^{k-1} x_i^n .$$

Na osnovu teoreme 3.3, odnosno jednakosti (3.19)-(3.23), koristeći Vietove veze, lako izračunavamo simetrične funkcije

$f_1, f_2, \ldots, f_5$. No, onda, nakon kraćeg računa, na osnovu poznatih veza izmedju s_n i simetričnih funkcija $f_1, f_2, \ldots f_n$, $n=1,2,\ldots 5$, dobijamo

$$s_1 = \frac{1}{2}(k-1), \quad s_2 = \frac{1}{12}(5k-7), \quad s_3 = \frac{1}{8}(3k-5),$$

$$s_4 = \frac{1}{720}(251k-469), \quad s_5 = \frac{1}{288}(95k-193).$$

Iz (4.25) sledi

$$-2k(k-1) + \ln A < -2k(k-1) - \sum_{n=1}^{5} \frac{s_n}{n} = -a(k-1)^2 - b(k-1) -$$

$$- c < -(a + \frac{b}{k-1})(k-1)^2, \qquad (4.26)$$

gde je $a=2,4358$; $b=1,77$; $c=0,08>0$.

Kako je po Stirling-ovoj formuli

$$k! < (\frac{k}{e})^k \sqrt{2\pi k}\, e^{(12k)^{-1}},$$

to iz (4.24), uzimajući u obzir (4.26), sledi

$$0 < |R_k| < k^{2k(k-1)} e^{-2k(k-1)} (2\pi k)^{k-1} e^{(k-1)(6k)^{-1}} e^{\ln A} <$$

$$< k^{(2k+1)(k-1)} (2\pi e (6k)^{-1})^{k-1} e^{-(a+b(k-1)^{-1})(k-1)^2} =$$

$$= \left[k^{(2k+1)(k-1)^{-1}} (2\pi e (6k)^{-1} - b)^{(k-1)^{-1}} e^{-a}\right]^{(k-1)^2} <$$

$$< \left[e^{-\lambda_k (2k+1)(k-1)^{-1}}\right]^{(k-1)^2}, \qquad (4.27)$$

gde je (s obzirom na $k \geq 14$)

$$(2\pi e (6k)^{-1} - b)^{(k-1)^{-1}} e^{-a} \leq (2\pi e 84^{-1} - b)^{13^{-1}} e^{-a} \leq e^{-\lambda}, \quad \lambda = 2,43.$$

Dokažimo da je za $k \geq 14$ ispunjena nejednakost

$$e^{-\lambda_k (2k+1)(k-1)^{-1}} < e^{\sqrt{k-1}}. \qquad (4.28)$$

Stvarno, stavljajući $f(k) = (k-1)\sqrt{k-1} - (2k+1)\ln k + \lambda(k-1)$, nalazimo $f'(k) = \frac{3}{2}\sqrt{k-1} + \lambda - 2 - \frac{1}{k} - 2\ln k$, pa funkcija $f(k)$ ima minimum za $k<8$. Sledi, za $k \geq 14$ funkcija $f(k)$ raste, tj.

$$f(k) \geq f(14) > \frac{3}{2} > 0.$$

No, onda je za svako $k \geq 14$ nejednakost (4.28) tačna, pa iz (4.27) sledi

$$0 < |R_k| < e^{(k-1)^2 \sqrt{k-1}}.$$

Po pretpostavci je $k \leq 2k_0 < 1 + \sqrt{\ln^2 p}$, pa izlazi

$$0 < |R_k| < e^{\ln p} = p. \qquad (4.29)$$

No, (4.29) je u kontradikciji sa (4.23), pa je time teorema u potpunosti dokazana.

Primetimo ovde, da teorema 4.3 predstavlja vrlo snažan kriterijum u prvom slučaju Fermat-ovog problema. Naime,prost broj p, koji bi zadovoljavao uslov da je k_o uzastopnih parnih Bernoulli-jevih brojeva,i to počevši od B_{p-3}, deljivo sa p, mora imati očigledno vrlo izuzetne "kvalitete". Do sada nije poznat nijedan takav broj p. Medju prostim brojevima ≤ 4001, takvoq nema.

4.3 Wieferich-ov rezultat

U odeljku 1.7 naveli smo, izmedju ostalog, rezultate niza matematičara, vezane za prvi slučaj Fermat-ovog problema,sažete u uslovu: jednačina (4.1) nema rešenja relativno prosta sa p, ako je

$$q^{p-1} \not\equiv 1 \pmod{p^2}, \quad 2 \leq q \leq 31, \quad q \in P.$$

Prvi od tih rezultata, u slučaju $q=2$, dao je Wieferich. Sada smo u mogućnosti da, koristeći osobine niza polinoma $D_k(x)$, dokažemo Wieferich-ov rezultat.

Lema 4.2 Neka je $p \in P$, $p \geq 3$, $n < p-1$, $n \in N$, i neka je

$$s_n = 1^n + 3^n + \ldots + p^n + (-1)^n (2^n + 4^n + \ldots + (p-1)^n).$$

Tada je

$$s_n \equiv \begin{cases} 0, & n \text{ parno} \\ \dfrac{2^{n+2} - 2}{n+1} B_{n+1}, & n \text{ neparno} \end{cases} \pmod{p}. \qquad (4.30)$$

Dokaz. Za n parno, (4.30) je neposredna posledica leme 1.17, pošto je

$$s_n = S_n(p) + p^n \equiv 0 \pmod{p}, \quad n=2k, \quad n<p-1.$$

Neka je n neparno. Imamo

$$s_n = 1^n - 2^n + 3^n - \ldots - (p-1)^n + p^n \equiv 1^n + 3^n + \ldots + p^n +$$
$$+ (p-2)^n + (p-4)^n + \ldots + 1^n \equiv 2(1^n + 3^n + \ldots + (p-2)^n) \equiv$$
$$\equiv -2(2^n + 4^n + \ldots + (p-1)^n) = -2^{n+1}[1^n + 2^n + \ldots +$$

$$+ \left(\frac{p-1}{2}\right)^n] = -2^{n+1} S_n\left(\frac{p+1}{2}\right) \pmod p. \qquad (4.31)$$

Koristeći leme 1.16 i 1.18 iz (4.31) sledi

$$e_n \equiv -2^{n+1}\frac{1}{n+1}(n+1)S_n\left(\frac{p+1}{2}\right) = -\frac{2^{n+1}}{n+1}[(\frac{p+1}{2}+B)^{n+1}-$$

$$-B_{n+1}] \equiv -\frac{2^{n+1}}{n+1}[(\frac{1}{2}+B)^{n+1}-B_{n+1}] = -\frac{2^{n+1}}{n+1}[(2^{-n}-$$

$$-1)B_{n+1}-B_{n+1}] = \frac{2^{n+2}-2}{n+1}B_{n+1} \pmod p,$$

što je i trebalo dokazati.

Teorema 4.4 Ako je .

$$2^{p-1} \not\equiv 1 \pmod{p^2}, \qquad (4.32)$$

tada jednačina (4.1) nema rešenja relativno prosta sa p.

Dokaz. Neka je

$$\alpha_n = \begin{cases} ts_n, & n \text{ parno} \\ (2-t)s_n, & n \text{ neparno} \end{cases}.$$

Tada je, na osnovu leme 4.2

$$\alpha_n \equiv \begin{cases} 0, & n \text{ parno} \\ \frac{2^{n+2}-2}{n+1}B_{n+1}(2-t), & n \text{ neparno} \end{cases} \pmod p. \qquad (4.33)$$

S druge strane, na osnovu leme 3.13, važi

$$[(p+1)t-1]D_k(t) = t^{k+1}s_k - [D(t)-\alpha t]^k. \qquad (4.34)$$

Uzimajući u obzir (4.33), iz (4.34) za $k=p-2$, sledi

$$D_{p-2}(t) \equiv (2-t)[\binom{p-2}{1}(2^2-1)B_2 D_{p-3}(t) +$$

$$+ \binom{p-2}{3}\frac{2^4-1}{2}t^2 B_4 D_{p-5}(t) + \ldots +$$

$$+ \binom{p-2}{p-4}\frac{2^{p-3}-1}{\frac{p-3}{2}}t^{p-5}B_{p-3}D_2(t)] + 2\frac{2^{p-1}-1}{\frac{p-1}{2}}t^{p-3}B_{p-1}$$

$$\pmod p, \qquad (4.35)$$

uz pretpostavku $t \not\equiv 0 \pmod p$.

Pretpostavimo obrnuto tvrdjenju teoreme: neka važi (4.32) i neka jednačina (4.1) ima rešenja relativno prosta sa p. Na osnovu teoreme 4.1, izmedju ostalog, važi za svako $k=2,4,\ldots p-3, p-2$

$$B_{p-k-1}D_k(t) \equiv 0 \pmod{p}, \tag{4.36}$$

gde je

$$t \equiv \frac{y}{z} \not\equiv 0 \pmod{p}.$$

Specijalno, za $k=p-2$, važi

$$D_{p-2}(t) \equiv 0 \pmod{p}. \tag{4.37}$$

Iz (4.35), (4.36) i (4.37) sledi

$$D_{p-2}(t) \equiv 2\,\frac{2^{p-1}-1}{\frac{p-1}{2}}\,t^{p-3}B_{p-1} \equiv 0 \pmod{p},$$

odnosno,

$$(2^{p-1}-1)B_{p-1} \equiv 0 \pmod{p}. \tag{4.38}$$

Prema teoremi 1.15 važi

$$pB_{p-1} \equiv -1 \pmod{p},$$

pa (4.38) daje

$$\frac{2^{p-1}-1}{p}\,pB_{p-1} \equiv -\frac{2^{p-1}-1}{p} \equiv 0 \pmod{p}, \text{ tj.}$$

$$2^{p-1} \equiv 1 \pmod{p^2},$$

što protivreči uslovu (4.32). Time je teorema u potpunosti dokazana.

Napomenimo ovde da su Brillhart, Tonascia i Weinberger, koristeći upravo rezultat Wieferich-a, pokazali 1971. godine u [3] da za $p < 3\cdot 10^9$ jednačina (4.1) nema rešenja relativno prosta sa p. Naime, medju svim prostim brojevima $<3\cdot 10^9$, samo dva, $p=1093$ i $p=3511$, zadovoljavaju uslov

$$2^{p-1} \equiv 1 \pmod{p^2}.$$

Medjutim, oba broja padaju pod udar drugih kriterijuma, na primer, za oba broja je

$$3^{p-1} \not\equiv 1 \pmod{p^2}.$$

4.4 Niz polinoma $D_k(t)$ i Bernoulli-jevi brojevi

Videli smo u prethodnim odeljcima koliku su ulogu u tretiranju prvog slučaja Fermat-ovog problema imali niz polinoma $D_k(t)$ i Bernoulli-jevi brojevi. Mi smo ih dosad tretirali nezavisno jedne od drugih. Medjutim, u prilici smo da pokažemo da su, niz polinoma $D_k(t)$ s jedne i Bernoulli-jevi brojevi s druge strane, neraskidivo vezani. To će, izmedju ostalog, omogućiti da se uslovi izraženi teoremama 4.3 i 4.4 stope u jedan jedini uslov. Postavimo to kao naš poslednji zadatak.

Teorema 4.5 Za svako $k \in N$ važi jednakost

$$B_{k+1} = \frac{k+1}{2^{k+1}(2^{k+1}-1)} D_k(2) \qquad (4.39)$$

Dokaz. Primetimo da je za k parno jednakost (4.39) očigledno tačna. Naime, prema lemi 3.10 je za k parno, $k \in N$, $D_k(2)=0=B_{k+1}$. Prema tome, dokaz se, u krajnjoj liniji, svodi na to da se jednakost (4.39) dokaže za neparne prirodne brojeve k.

Uočimo funkciju $y=tgx$ i razvijmo je u stepeni red po stepenima od x. Imamo

$$tgx = \frac{\sin x}{\cos x} = \frac{e^{ix}-e^{-ix}}{i(e^{ix}+e^{-ix})} = \frac{(e^{2ix}-1)^2}{i(e^{4ix}-1)} = \frac{1}{i}\left(1 - \frac{2}{e^{2ix}-1} + \frac{4}{e^{4ix}-1}\right) = \frac{1}{x}\left(-ix + \frac{2ix}{e^{2ix}-1} - \frac{4ix}{e^{4ix}-1}\right) =$$

$$= \frac{1}{x}\left(-ix + \sum_{m=1}^{\infty} \frac{B_m(2ix)^m}{m!} - \sum_{m=1}^{\infty} \frac{B_m(4ix)^m}{m!}\right) =$$

$$= \frac{1}{x}\left(\sum_{m=2}^{\infty} \frac{B_m(2ix)^m}{m!} - \sum_{m=2}^{\infty} \frac{B_m(4ix)^m}{m!}\right) =$$

$$= \sum_{m=2}^{\infty} \frac{(2i)^m(1-2^m)B_m x^{m-1}}{m!} =$$

$$= \sum_{m=1}^{\infty} \frac{(-1)^{m-1}2^{2m}(2^{2m}-1)B_{2m}}{(2m)!} x^{2m-1} \qquad (4.40)$$

S druge strane funkcija $y=tgx$ zadovoljava jednakost

$$y' \sin 2x = 2y. \tag{4.41}$$

Neka je (funkcija $y = tgx$ je neparna)

$$tgx = \sum_{m=1}^{\infty} \frac{a_{2m-1}}{(2m-1)!}\, x^{2m-1}. \tag{4.42}$$

Red (4.42) je u izvesnoj okolini nule (na primer, u $[-1,1]$) uniformno konvergentan, pa iz (4.41) sledi

$$\left(\sum_{m=1}^{\infty} \frac{a_{2m-1}}{(2m-2)!}\, x^{2m-2}\right)\left(\sum_{m=1}^{\infty} \frac{(-1)^{m-1} 2^{2m-1}}{(2m-1)!}\, x^{2m-1}\right) =$$

$$= \sum_{m=1}^{\infty} \frac{2a_{2m-1}}{(2m-1)!}\, x^{2m-1}.$$

Množenjem redova na levoj strani gornje jednakosti i uporedjivanjem koeficijenata uz x^{2m-1} dobijamo

$$\frac{2a_{2m-1}}{(2m-2)!1!} - \frac{2^3 a_{2m-3}}{(2m-4)!3!} + \ldots + \frac{(-1)^{m-1} 2^{m-1} a_1}{(2m-1)!} = \frac{2a_{2m-1}}{(2m-1)!},$$

odnosno, nakon sredjivanja

$$2a_{2m-1} = \binom{2m-1}{1} 2a_{2m-1} - \binom{2m-1}{3} 2^3 a_{2m-3} + \ldots +$$

$$+ (-1)^{m-1} \binom{2m-1}{2m-1} 2^{2m-1} a_1 = \left[\binom{2m}{1} 2a_{2m-1} - \binom{2m}{3} 2^3 a_{2m-3} + \right.$$

$$\left. + \ldots + (-1)^{m-1} \binom{2m}{2m-1} 2^{2m-1} a_1\right] - 2\left[\binom{2m-1}{0} a_{2m-1} - \right.$$

$$\left. - \binom{2m-1}{2} 2^2 a_{2m-3} + \ldots + (-1)^{m-1} \binom{2m-1}{2m-2} 2^{2m-2} a_1\right]. \tag{4.43}$$

S druge strane, prema lemi 3.7 važi

$$D_k(t) = (1-t)\left[D(t)+t\right]^k + t^{k+1},$$

odnosno za $t=2$

$$D_k(2) = 2^{k+1} - \left[D(2)+2\right]^k. \tag{4.44}$$

Vodeći računa da je $D_{2m}(2)=0$ za svako $m \in N$, iz (4.44) sledi

$$2D_{2m-1}(2) = 2D_{2m-1}(2) - D_{2m}(2) = 2\left[2^{2m} - (D(2)+2)^{2m-1}\right] -$$

$$- \left[2^{2m+1} - (D(2)+2)^{2m}\right] = -2\left[D_{2m-1}(2) + \binom{2m-1}{2} 2^2 D_{2m-3}(2) + \right.$$

$$\left. + \ldots + \binom{2m-1}{2m-2} 2^{2m-2} D_1(2) + 2^{2m-1}\right] + \left[\binom{2m}{1} 2D_{2m-1}(2) + \right.$$

$$+ \binom{2m}{3} 2^3 D_{2m-3}(2) + \ldots + \binom{2m}{2m-1} 2^{2m-1} D_1(2) + 2^{2m}],$$

odnosno, množenjem sa $(-1)^{m-1}$ izlazi

$$2(-1)^{m-1} D_{2m-1}(2) = -2[(-1)^{m-1} D_{2m-1}(2) -$$

$$- \binom{2m-1}{2} 2^2 (-1)^{m-2} D_{2m-3}(2) + \ldots +$$

$$+ \binom{2m-1}{2m-2} (-1)^{m-1} 2^{2m-2} D_1(2)] + [\binom{2m}{1} 2(-1)^{m-1} D_{2m-1}(2) -$$

$$- \binom{2m}{3} 2^3 (-1)^{m-2} D_{2m-3}(2) + \ldots + \binom{2m}{2m-1} (-1)^{m-1} 2^{2m-1} D_1(2)].$$

Drugim rečima, niz $(-1)^{m-1} D_{2m-1}(2)$ zadovoljava jednakost (4.43). Kako je uz to $a_1 = 1 = D_1(2)$, to zaključujemo da je za svako $m \in N$

$$a_{2m-1} = (-1)^{m-1} D_{2m-1}(2). \qquad (4.45)$$

Uzimajući u obzir (4.40), (4.42) i (4.45) izlazi

$$D_{2m-1}(2) = \frac{2^{2m}(2^{2m}-1)}{2m} B_{2m},$$

pa je jednakost (4.39) tačna i za sve neparne prirodne brojeve k. Time je teorema u potpunosti dokazana.

Primetimo, da je neposredna posledica jednakosti (4.39) poznata osobina Bernoulli-jevih brojeva da su svi prosti faktori imenioca broja B_{2k} delitelji broja $2(2^{2k}-1)$. Postojeći dokaz ove osobine je, inače, mnogo komplikovaniji ([18], 264-269).

Nas, medjutim, interesuje najviše kako se jednakost (4.39) odražava na teoremama 4.3 i 4.4. Praktično, bez ikakvih poteškoća, u stanju smo da dokažemo sledeću teoremu.

Teorema 4.6 Ako je bar za jedno k, $k=2,4,\ldots,2k_o$, $k_o = max\,(7, \left[\frac{1}{2}(3 + \sqrt[5]{ln^2 p})\right])$, ispunjeno

$$D_{p-k}(2) \not\equiv 0 \pmod{p}, \qquad (4.46)$$

tada jednačina (4.1) nema rešenja relativno prosta sa p.

Dokaz. Neka je $p \neq 3,5,7,11,13,19,41,43,223,2731,36389,75571,20579903$ i neka važi suprotno, tj. neka važi (4.46) i neka jednačina (4.1) ima rešenja relativno prosta sa p. Prema teoremi 4.3, uzimajući u obzir jednakost (4.39), mora biti

$$D_{p-k}(2) \equiv 0 \pmod{p},$$

za svako $k=4,6,\ldots,2k_o$. No, onda je

$$D_{p-2}(2) \not\equiv 0 \pmod{p}. \tag{4.47}$$

Kako je

$$D_{p-2}(2) = \frac{2^{p-1}(2^{p-1}-1)}{p-1} B_{p-1} = \frac{2^{p-1}}{p-1} \cdot \frac{2^{p-1}-1}{p} pB_{p-1},$$

to iz (4.47), na osnovu teoreme 1.15, sledi

$$2^{p-1}-1 \not\equiv 0 \pmod{p^2},$$

što protivreči tvrdjenju teoreme 4.4.

Preostalo je da se teorema dokaže za izuzete vrednosti p. Kako je za sve takve vrednosti p ispunjeno

$$2^{p-1} \not\equiv 1 \pmod{p^2},$$

odnosno,

$$D_{p-2}(2) \not\equiv 0 \pmod{p^2},$$

to je teorema u potpunosti dokazana.

4.5 Umesto zaključka

Dobar je običaj da se na kraju svakog izlaganja kraćim zaključkom pogase svetla na pozornici posmatranih događjaja. No, šta zaključiti na kraju izlaganja o problemu,koji je bio i ostao nerešen? Reći da je Fermat imao, ili nije imao pravo, ne možemo. Reći da Fermat verovatno nije raspolagao tačnim dokazom svog tvrdjenja, nesvrsishodno je. Reći da će neko jednog dana staviti kakvu takvu tačku na Fermat-ov problem, očigledno je.

I zato, umesto zaključka, recimo samo to, da je Fermat-ov problem, nezavisno od toga koliko je objektivno značajan, bio i biće jedan od povoda da se u matematici stvara, da se u matematici i sa matematikom ide napred. Zbog toga, izreka "da nerešenih problema u matematici nema, trebalo bi ih izmisliti", izgleda, i nije samo duhovita.

L I T E R A T U R A

1. Ahmad S.
   Algebraic Domains and Fermat´s Last Theorem,
   Notices of the American Mathematical Society 20 (1973), 629.

2. Боревич З.И., Шафаревич И.Р.
   Теория чисел, Москва, 1964.

3. Brillhart J., Tonascia J. and Weinberger R.
   On the Fermat quotient,
   Computers in Number Theory (1971), 213-222.

4. Brückner H.
   Zum Beweis des ersten Falles der Fermatschen Vermutung für pseudoreguläre Primzahlen l,
   Journal für die reine und angewandte Mathematik 253 (1972), 15-18.

5. Brückner H.
   Zum ersten Fall der Fermatschen Vermutung,
   Journal für die reine und angewandte Mathematik 274/275 (1975), 21-26.

6. Бухштаб А.А.
   Теория чисел, Москва, 1966.

7. Dickson L.E.
   History of the Theory of Numbers I-III, Washington, 1920.

8. Dickson L.E.
   Introduction to the Theory of Numbers, Chicago, 1931.

9. Edwards H.M.
   Background of Kummer´s Proof of Fermat´s Last Theorem for Regular Primes,
   Archive for History of Exact Sciences 14 (1975), 219-236.

10. Eichler M.
Eine Bemerkung zur Fermatschen Vermutung,
Acta Arithmetica 11 (1965), 129-131.

11. Eichler M.
Zum ersten Fall der Fermatshen Vermutung,
Journal für die reine und angewandte Mathematik 253
(1972), 19.

12. Everett C.J.
Fermat's conjecture, Roth's theorem, Pythagorean
triangles and Pell's equation,
Duke Mathematical Journal 40 (1973), 801-804.

13. Frobenius G.
Über den Fermatschen Satz III,
Sitzungsberichte der Akademie der Wissenschaften 123,
Berlin (1914), 653-681.

14. Furtwängler Ph.
Letzter Fermatscher Satz und Eisensteinsches
Reziprozitätsprinzip,
Sitzungsberichte der Akademie der Wissenschaften 121,
Wien (1912), 589-592.

15. Gandhi J.M.
On Fermat's Last Theorem,
The American Mathematical Monthly 71 (1964), 998-1006.

16. Gandhi J.M.
On Fermat's last theorem,
Journal für die reine and angewandte Mathematik 250
(1971), 49-55.

17. Gandhi J.M., Patel B.G.
On Fermat's last theorem,
Journal für die reine und angewandte Mathematik 286/287
(1976), 196-204.

18. Гельфонд А.О.
Исчисление конечных разностей, Москва, 1967.

19. Gould H.W.
Explicit Formulas for Bernoulli Numbers,
The American Mathematical Monthly 79 (1972), 44-51.

20. Inkeri K.
A note on Fermat's conjecture,
Acta Arithmetica 29 (1976), 251-256.

21. Inkeri K. and Hyyrö S.
Über die Anzahl der Lösungen einiger Diophantischer Gleichungen,
Annales Univ. Turku 78 (1964), 3-10.

22. Krasner M.
Sur le premier cas du theoreme de Fermat,
Comptes Rendus de l'Academie des Sciences 199 (1934), 256-258.

23. Krasner M.
A propos du critere de Sophie Germain-Furtwängler pour le premier du theoreme de Fermat,
Mathematica 16, Cluj (1940), 109-114.

24. Kurepa Dj.
Viša algebra I i II, Zagreb, 1965.

25. Kurepa Dj.
On the left factorial function $!n$,
Mathematica Balcanica 1 (1971), 147-153.

26. Курош А.Г.
Курс высшей алгебры, Москва, 1971.

27. Курош А.Г.
Лекции по общей алгебре, Москва, 1973.

28. Landau E.
Vorlesungen über Zahlentheorie III, Leipzig, 1927.

29. Le Veque W.J.
Topics in Number Theory II, Massachusetts, 1961.

30. Lehmer D.H.
A Factorization Theorem Applied to a Test for Primality,
Bulletin of American Mathematical Society 45 (1939),
132-137.

31. Lehmer D.H.
The Lattice Points of an n-Dimensional Tetrahedron,
Duke Mathematical Journal 7 (1940), 341-353.

32. Lehmer D.H. Lehmer Emma
On the First Case of Fermat´s Last Theorem,
Bulletin of American Mathematical Society 47 (1941),
139-142.

33. Mahoney M.S.
Fermat´s Mathematics: Proofs and Conjectures,
Science 178 (1972), 30-36.

34. Mc Donnel J.
New Criteria Associated with Fermat´s Last Theorem,
Bulletin of American Mathematical Society 36 (1930),
553-558.

35. Mirimanoff D.
Sur le dernier theoreme de Fermat,
Comptes Rendus de l´Academie des Sciences 150 (1910),
204-206.

36. Mitrinović D.S., Marsh D.C.B.
Problemi iz elementarne teorije brojeva, Beograd, 1965.

37. Mordell L.J.
Three Lectures on Fermat´s Last Theorem, Cambridge, 1920.

38. Mordell L.J.
Diophantine Equations, London and New York, 1969.

39. Morishima T.
Über den Fermatschen Quetienten,
Japanese Journal of Mathematics 8 (1931), 159-173.

40. Онигова Е.П.
Развитие теории чисел в России, Ленинград, 1972.

41. Perisastri M.
A note on Fermat's Last Theorem,
The American Mathematical Monthly 75 (1968).

42. Perisastri M.
On Fermat's last theorem II,
Journal für die reine und angewandte Mathematik 265 (1974), 142-144.

43. Polaczek F.
Über den grossen Fermat'schen Satz,
Sitzungsberichte der Akademie der Wissenschaften 126 (1917), 25-59.

44. Ribenboim P.
Algebraic Numbers, Wiley,1972.

45. Ribenboim P.
Lecture - Recent Results ou Fermat's Last Theorem,
Canad. Math. Bull. 20(2) (1977), 229-242.

46. Rosser J.B.
On the First Case of Fermat's Last Theorem,
Bulletin of American Mathematical Society 45 (1939), 636-640.

47. Rosser J.B.
A New Lower Bund for the Exponent in the First Case of Fermat's Last Theorem,
Bulletin of American Mathematical Society 46 (1940), 299-304.

48. Rosser J.B.
An Aditional Criterion for the First Case of Fermat's Last Theorem,
Bulletin of American Mathematical Society 47 (1941), 109-110.

49. Rotkiewicz A.
Sur les nombres de Mersenne depourvus de diviseurs carres et sur les nombres naturels n tels ques $n^2 | 2^n - 2$,
Matematicky Vesnik 17 (1965), 78-80.

50. Skula L.
Eine Bemerkung zu dem ersten Fall der Fermatschen Vermutung,
Journal für die reine und angewandte Mathematik 253 (1972), 1-14.

51. Šami Z.
O Fermat-ovom problemu,
magistarski rad, Beograd, 1973.

52. Šami Z.
On the M-hypothesis of Dj. Kurepa,
Mathematica Balcanica 3 (1973), 530-532.

53. Vandiver H.S.
Extension of the criteria of Wieferich and Mirimanoff in connection with Fermat's last theorem,
Journal für die reine und angewandte Mathematik 144 (1914), 314-318.

54. Vandiver H.S.
A property of cyclotomic integers and its relation to Fermat's last theorem,
Annals of Mathematics 21 (1919), 73-80.

55. Vandiver H.S.
Note on trinomial congruences and the first case of the Fermat's last theorem,
Annals of Mathematics 27 (1926), 54-56.

56. Vandiver H.S.
On Fermat's Last Theorem,
Trans. Amer. Math. Soc. 31 (1929), 613-642.

57. Vandiver H.S.
Fermat's Last Theorem and the Second Factor in the Cyclotomic Class Number,
Bulletin of the American Mathematical Society 40 (1934), 118-126.

58. Vandiver H.S.
Fermat's Last Theorem,
The American Mathematical Monthly 53 (1946), 555-578.

59. Vandiver H.S.
A Supplementary Note to a 1946 Article on Fermat's Last Theorem,
The American Mathematical Monthly 60 (1953), 164-167.

60. Vandiver H.S.
New Types of Trinomial Congruence Criteria Applying to Fermat's Last Theorem,
Proc. Nat. Acad. Sci. USA 40 (1954), 248-252.

61. Vandiver H.S.
Examination of Methods of Attack on the Second Case of Fermat's Last Theorem,
Proc. Nat. Acad. Sci. USA 40 (1954), 732-735.

62. Виноградов И.М.
Основы теории чисел, Москва, 1972.

63. Wieferich A.
Zum letzten Fermatschen Theorem,
Journal für die reine und angewandte Mathematik 136 (1909), 293-302.

S A D R Ž A J