W każdym więc razie ideał $[p]$ jest podzielny przez $\mathfrak{p}$ na mocy twierdzenia 10.

Zbadamy obecnie, jak rozkładają się na ideały pierwsze ideały $[p]$, gdzie p jest liczbą pierwszą wymierną.

Okażemy najpierw, że $[p]$ nie może być iloczynem trzech ideałów, z których każdy jest różny od $[1]$.

Istotnie, przypuśćmy, że $[p]=\mathfrak{i}_1\cdot\mathfrak{i}_2\cdot\mathfrak{i}_3$, gdzie żaden z ideałów $\mathfrak{i}_1, \mathfrak{i}_2, \mathfrak{i}_3$ nie jest ideałem $[1]$. Zatem $\mathfrak{N}(\mathfrak{i}_1)>1$, $\mathfrak{N}(\mathfrak{i}_2)>1$ i $\mathfrak{N}(\mathfrak{i}_3)>1$, skąd wobec $\mathfrak{N}([p])=p^2$ wynika rozkład

$$p^2=\mathfrak{N}(\mathfrak{i}_1)\cdot\mathfrak{N}(\mathfrak{i}_2)\cdot\mathfrak{N}(\mathfrak{i}_3),$$

co niemożliwe.

Tak więc ideał główny $[p]$, gdzie p jest liczbą pierwszą wymierną, jest albo ideałem pierwszym, albo iloczynem dwu ideałów pierwszych.

Okażemy obecnie, że jeżeli ideał główny $[p]$, gdzie p jest liczbą pierwszą wymierną, jest iloczynem dwu ideałów pierwszych, to ideały te są sprzężone.

Istotnie, jeżeli $[p]=\mathfrak{p}_1\mathfrak{p}_2$, gdzie $\mathfrak{p}_1$ i $\mathfrak{p}_2$ są ideałami pierwszymi, to $\mathfrak{N}([p])=\mathfrak{N}(\mathfrak{p}_1)\cdot\mathfrak{N}(\mathfrak{p}_2)$, czyli wobec $\mathfrak{N}([p])=p^2$

$$p^2=\mathfrak{N}(\mathfrak{p}_1)\cdot\mathfrak{N}(\mathfrak{p}_2).$$

Ponieważ zaś każda z liczb $\mathfrak{N}(\mathfrak{p}_1)$ i $\mathfrak{N}(\mathfrak{p}_2)$ jest większa od 1, więc $\mathfrak{N}(\mathfrak{p}_1)=p$ i $\mathfrak{N}(\mathfrak{p}_2)=p$, skąd

$$[\mathfrak{N}(\mathfrak{p}_1)]=[p].$$

Ponieważ wreszcie $N(\mathfrak{p}_1)=[\mathfrak{N}(\mathfrak{p}_1)]$ i zarazem $N(\mathfrak{p}_1)=\mathfrak{p}_1\cdot\mathfrak{p}_1'$, więc ostatecznie

$$[p]=\mathfrak{p}_1\cdot\mathfrak{p}_1'.$$

Możemy zatem wypowiedzieć następujące

Twierdzenie 16. *Jeżeli p jest liczbą pierwszą wymierną, to ideał $[p]$ jest albo ideałem pierwszym, albo kwadratem ideału pierwszego, albo wreszcie iloczynem dwu różnych ideałów pierwszych sprzężonych.*

Z wniosku z twierdzenia 15 wynika, że dla wyznaczenia wszystkich ideałów pierwszych danego ciała liczbowego $K(\sqrt{D})$ wystarczy wyznaczyć czynniki pierwsze ideałów $[p]$, gdzie p jest liczbą pierwszą wymierną.

ROZDZIAŁ XIX

WIELKIE TWIERDZENIE FERMATA DLA WYKŁADNIKÓW 5 i 7

§ 1. Ciała liczbowe, w których każdy ideał jest główny. Udowodnimy najpierw ogólnie następujący

Lemat I. *Jeżeli w ciele liczbowym $K(\sqrt{D})$ warunki*

$$|u|\leqslant{}^1/_2, \qquad |v|\leqslant{}^1/_2 \tag{1}$$

pociągają za sobą zawsze warunek

$$|N(u+v\omega)|<1, \tag{2}$$

to każdy ideał ciała $K(\sqrt{D})$ jest ideałem głównym.

Dowód. Niech $\mathfrak{i}$ będzie ideałem w ciele $K(\sqrt{D})$. Dla każdej liczby $\lambda\neq 0$ ideału $\mathfrak{i}$ utwórzmy liczbę $|N(\lambda)|$. Jest to liczba naturalna. Niech n będzie najmniejszą z tych wszystkich liczb. Istnieje więc taka liczba λ_0 należąca do $\mathfrak{i}$, że $|N(\lambda_0)|=n$.

Okażemy, że

$$\mathfrak{i}=[\lambda_0].$$

Istotnie, niech

$$\lambda_0=u_0+v_0\omega,$$

gdzie u_0 i v_0 są liczbami całkowitymi wymiernymi i niech $\lambda=u+v\omega$ będzie jakąkolwiek liczbą ideału $\mathfrak{i}$. Ponieważ $n=|N(\lambda_0)|>0$, więc $\lambda_0\neq 0$. Iloraz λ/λ_0, jako liczba ciała $K(\sqrt{D})$, może być przedstawiony w formie

$$\lambda/\lambda_0=x+y\omega, \tag{3}$$

gdzie x i y są liczbami rzeczywistymi wymiernymi. Możemy dalej wyznaczyć takie liczby całkowite wymierne a i b, że

$$|x-a|\leqslant{}^1/_2 \quad \text{i} \quad |y-b|\leqslant{}^1/_2. \tag{4}$$

Niech

$$x-a=\xi \quad \text{i} \quad y-b=\eta.$$

Zatem w myśl (3) jest $\lambda/\lambda_0 = a + b\omega + \xi + \eta\omega$ czyli

(5) $$\lambda = \lambda_0(a + b\omega) + \beta,$$

gdzie

(6) $$\beta = \lambda_0(\xi + \eta\omega).$$

Równość (5) wskazuje, że $\beta = \lambda - \lambda_0(a + b\omega)$ jest liczbą całkowitą ciała $K(\sqrt{D})$. Równość zaś (6) daje

(7) $$|N(\beta)| = |N(\lambda_0)| \cdot |N(\xi + \eta\omega)|,$$

a że na mocy (4) jest $|\xi| \leqslant {}^1/_2$ i $|\eta| \leqslant {}^1/_2$, więc, w myśl założenia lematu musi być $|N(\xi + \eta\omega)| < 1$, skąd wobec $|N(\lambda_0)| > 0$, otrzymujemy z (7) nierówność $|N(\beta)| < |N(\lambda_0)|$, która, na mocy określenia liczby n, zachodzić może tylko dla $\beta = 0$.

Dowiedliśmy więc, że $\beta = 0$, skąd $\lambda = \lambda_0(a + b\omega)$ na mocy (5). Wobec całkowitości liczby $a + b\omega$, wynika stąd, że λ jest liczbą ideału $[\lambda_0]$. Każda liczba ideału $\mathfrak{i}$ należy więc do ideału $[\lambda_0]$. Ale i na odwrót, gdyż λ_0 należy do $\mathfrak{i}$. Tak więc $\mathfrak{i} = [\lambda_0]$, c. b. d. o.

Wniosek 1. *Każdy ideał ciała $K(\sqrt{-1})$ jest ideałem głównym.*

Jest tu bowiem $N(u + v\omega) = u^2 + v^2$, zatem nierówność (1) daje

$$|N(u + v\omega)| \leqslant {}^1/_4 + {}^1/_4 = {}^1/_2 < 1.$$

Wniosek 2. *Każdy ideał ciała $K(\sqrt{-3})$ jest ideałem głównym.*

Jest tu bowiem $N(u + v\omega) = u^2 + uv + v^2$, a zatem nierówność (1) daje

$$|N(u + v\omega)| \leqslant {}^1/_4 + {}^1/_4 + {}^1/_4 = {}^3/_4 < 1.$$

Wniosek 3. *Każdy ideał ciała $K(\sqrt{5})$ jest ideałem głównym.*

Jest tu bowiem $N(u + v\omega) = u^2 + uv - v^2$, a zatem nierówność (1) daje

$$|N(u + v\omega)| \leqslant {}^3/_4 < 1.$$

§ 2. Twierdzenie Fermata dla potęgi $n = 5$. Udowodnimy z kolei

Lemat II. *Jeżeli suma $x^2 + y^2 + z^2$ jest podzielna przez 5 to co najmniej jedna z liczb x, y, z jest podzielna przez 5.*

Dowód. Przypuśćmy, że żadna z liczb x, y, z nie jest podzielna przez 5. Kwadrat liczby niepodzielnej przez 5 jest — jak łatwo widzieć — formy $5k \pm 1$. Z kongruencji $x^2 + y^2 + z^2 \equiv 0 \pmod 5$ wynikałoby więc, że $\pm 1 \pm 1 \pm 1 \equiv 0 \pmod 5$. Jest to jednak niemożliwe przy żadnej kombinacji znaków + i —, c. b. d. o.

Lemat III. *Jeżeli liczby całkowite wymierne x, y, z spełniają równanie*

(8) $$x^5 + y^5 + z^5 = 0,$$

to co najmniej jedna z nich jest podzielna przez 5.

Dowód. Z równania (8) wynika na mocy małego twierdzenia Fermata, że

$$x + y + z \equiv x^5 + y^5 + z^5 \equiv 0 \pmod 5,$$

zatem

$$(x + y + z)^5 = 5^5 t,$$

skąd na mocy tożsamości

$$2[(x + y + z)^5 - (x^5 + y^5 + z^5)] =$$
$$= 5(x + y)(y + z)(z + x)[(x + y + z)^2 + x^2 + y^2 + z^2]$$

oraz wobec (8) otrzymujemy równość

$$(x + y)(y + z)(z + x)[(x + y + z)^2 + x^2 + y^2 + z^2] = 5^4 2t.$$

Ponieważ zaś

$$x + y \equiv -z \pmod 5, \qquad y + z \equiv -x \pmod 5, \qquad z + x \equiv -y \pmod 5$$

oraz

$$(x + y + z)^2 \equiv 0 \pmod 5,$$

więc otrzymana równość daje

(9) $$xyz(x^2 + y^2 + z^2) \equiv 0 \pmod 5.$$

Otóż gdyby żadna z liczb x, y, z nie była podzielna przez 5, to na mocy lematu II mielibyśmy $x^2 + y^2 + z^2 \not\equiv 0 \pmod 5$, wbrew (9).

Tym samym lemat III jest dowiedziony.

W § 1 dowiedliśmy (p. wniosek 3), że każdy ideał ciała $K(\sqrt{5})$ jest główny. Udowodnimy jeszcze

Lemat IV. *Każdy ideał $\mathfrak{i}$ ciała $K(\sqrt{5})$ daje się przedstawić w postaci*

$$[a + b\sqrt{5}],$$

gdzie a i b są liczbami całkowitymi wymiernymi.

Dowód. Każdą liczbę całkowitą ciała $K(\sqrt{5})$ można przedstawić w formie

$$u+v\omega=u+v\frac{1+\sqrt{5}}{2}=\frac{2u+v+v\sqrt{5}}{2}.$$

W razie v parzystego dowód lematu jest natychmiastowy. Załóżmy więc, że v jest nieparzyste. Rozróżnimy dwa przypadki:

1° u jest nieparzyste. Wówczas, jak łatwo widzieć,

$$N(\omega)=N\left(\frac{1+\sqrt{5}}{2}\right)=-1,$$

zatem $\mathfrak{i}=[u+v\omega]=[\omega(u+v\omega)]$, gdzie

$$\omega(u+v\omega)=\frac{u+3v+(u+v)\sqrt{5}}{2}$$

i liczby $u+3v$ oraz $u+v$ są już parzyste.

2° u jest parzyste. Ponieważ $N(\omega')=N(\omega)=-1$, więc $\mathfrak{i}=[\omega'(u+v\omega)]$, gdzie

$$\omega'(u+v\omega)=\omega'u+vN(\omega)=\omega'u-v=\frac{1-\sqrt{5}}{2}u-v,$$

a ponieważ $u=2t$, więc $\mathfrak{i}=[t-v-t\sqrt{5}]$.

Twierdzenie 1. *Równanie*

(10) $$x^5+y^5=z^5$$

nie jest rozwiązalne w liczbach całkowitych wymiernych, różnych od zera.

Dowód. Przypuśćmy, że równanie (10) jest spełnione przez liczby całkowite x, y, z różne od zera. Na mocy lematu III jedna z tych liczb, np. z, musi zatem być podzielna przez 5. Niech

(11) $$z=5t;$$

możemy nadto założyć, że x, y i z, a więc też x i y nie mają wspólnego dzielnika większego od 1. Rozróżnimy dwa przypadki:

1° z jest parzyste. Liczby x i y są więc nieparzyste i można napisać

$$x+y=2p, \qquad x-y=2q,$$

skąd

(12) $$x=p+q, \qquad y=p-q;$$

wobec założenia, że $(x,y)=1$, jest również

(13) $$(p,q)=1.$$

Na mocy pierwszej z równości (12) jedna z liczb p i q jest parzysta, a druga nieparzysta. Wnosząc (12) do równania (10), dostajemy wobec założenia (11)

(14) $$x^5+y^5=2p(p^4+10p^2q^2+5q^4)=5^5t^5,$$

skąd wobec $z\neq 0$

(15) $$p\neq 0.$$

Musi być $p\equiv 0 \pmod 5$, ponieważ w przeciwnym razie byłoby $p^4+10p^2q^2+5q^4\not\equiv 0 \pmod 5$ i środkowa część wzoru (14) byłaby niepodzielna przez 5, co niemożliwe. Niech więc

(16) $$p=5r,$$

gdzie r jest liczbą całkowitą; wobec (15) jest też

(17) $$r\neq 0.$$

Wnosząc (16) do równości (14), dostajemy po podzieleniu przez 5^2

(18) $$2r(5^3r^4+2\cdot 5^2r^2q^2+q^4)=5^3t^5.$$

Okażemy, że oba czynniki lewej strony tej równości są względnie pierwsze. Istotnie, na mocy (13) i (16) jest

(19) $$(r,q)=1$$

jako też

(20) $$q\not\equiv 0 \pmod 5.$$

Mamy wobec (12) $p^4+10p^2q^2+5q^4\equiv p+q \pmod 2\equiv x \pmod 2$, a przeto wobec nieparzystości liczby x

(21) $$p^4+10p^2q^2+5q^4\equiv 1 \pmod 2;$$

ponieważ zaś $t\equiv 0 \pmod 2$ na mocy (14), więc wobec (21)

(22) $$p\equiv 0 \pmod 2,$$

skąd wobec (13)

(23) $$q\not\equiv 0 \pmod 2.$$

Z (16) i (22) wnosimy, że

(24) $$r\equiv 0 \pmod 2,$$

a przeto na mocy (23) ostatni czynnik lewej strony równości (18) jest nieparzysty. Wynika stąd, że każdy wspólny dzielnik h liczb $2r$ i $5^3r^4+2\cdot 5^2r^2q^2+q^4$ jest nieparzysty. Niech h będzie ich wspól-

nym dzielnikiem pierwszym. Zatem $h|r$ i $h|5^3r^4+2\cdot 5^2r^2q^2+q^4$, skąd wynika na mocy tożsamości

$$q^4=(5^3r^4+2\cdot 5^2r^2q^2+q^4)-(5^3r^2+2\cdot 5^2q^2)r^2,$$

że liczba pierwsza h jest dzielnikiem liczby q, a zatem wspólnym dzielnikiem liczb r i q. Na mocy (19) jest przeto $h=1$.

Tak więc okazaliśmy, że

$$(2r,\ 5^3r^4+2\cdot 5^2r^2q^2+q^4)=1. \tag{25}$$

Na mocy równości (20) ostatni czynnik jej lewej strony jest niepodzielny przez 5; wobec (18) i (25) czynniki te są więc postaci

$$2r=5^3a^5, \qquad 5^3r^4+2\cdot 5^2r^2q^2+q^4=b^5, \tag{26}$$

gdzie a i b są całkowite wymierne.

Ostatnią równość możemy też napisać w postaci

$$(q^2+5^2r^2)^2-5(10r^2)^2=b^5,$$

lub, przyjmując oznaczenia

$$P=q^2+5^2r^2 \quad \text{i} \quad Q=10r^2, \tag{27}$$

w postaci

$$P^2-5Q^2=b^5. \tag{28}$$

Na mocy (27) jest

$$P\equiv q+r \pmod 2 \quad \text{i} \quad P\equiv q^2 \pmod 5.$$

Pierwsza z tych kongruencji dowodzi wobec (23) i (24), że

$$P\not\equiv 0 \pmod 2, \tag{29}$$

druga zaś wobec (20), że

$$P\not\equiv 0 \pmod 5. \tag{30}$$

Okażemy, że

$$(P, Q)=1. \tag{31}$$

Istotnie, jeżeli h jest wspólnym dzielnikiem pierwszym liczb P i Q, to według (29) i (30) musi być $h\neq 2$ i $h\neq 5$. Pierwsza z równości (27) pociąga więc wobec $h|Q$, że $h|r$, skąd wywnioskowalibyśmy na mocy pierwszej z równości (25), że $h|q$. Na mocy (19) jest zatem $h=1$ i tym samym wzór (31) jest udowodniony.

Na mocy (28) jest

$$[P+Q\sqrt{5}][P-Q\sqrt{5}]=[b]^5. \tag{32}$$

Okażemy, że ideały, stojące po lewej stronie tej równości, są względnie pierwsze. Istotnie, przypuśćmy, że

$$[P+Q\sqrt{5}]=[\lambda_1][\lambda_0] \quad \text{i} \quad [P-Q\sqrt{5}]=[\lambda_2][\lambda_0],$$

gdzie $\lambda_0, \lambda_1, \lambda_2$ są liczbami całkowitymi ciała $K(\sqrt{5})$ oraz $[\lambda_0]\neq[1]$. Byłoby więc

$$P+Q\sqrt{5}=\varepsilon_1\lambda_1\lambda_0 \quad \text{i} \quad P-Q\sqrt{5}=\varepsilon_2\lambda_2\lambda_0,$$

gdzie ε_1 i ε_2 są dzielnikami jedności w tym ciele. Zatem

$$2P=(\varepsilon_1\lambda_1+\varepsilon_2\lambda_2)\lambda_0 \quad \text{i} \quad P^2-5Q^2=\varepsilon_1\varepsilon_2\lambda_1\lambda_2\lambda_0^2,$$

skąd wynika, że liczby $2P$ i P^2-5Q^2 należą do ideału $[\lambda_0]$. Ideał ten, różny od [1], byłby więc wspólnym dzielnikiem ideałów $[2P]$ i $[P^2-5Q^2]$. Na mocy twierdzenia 9 Rozdziału XVIII (§ 5, str. 457) liczby całkowite wymierne $2P$ i P^2-5Q^2 nie byłyby więc względnie pierwsze. Niech h będzie wspólnym dzielnikiem pierwszym tych liczb. Ze wzorów (27), (29) i (30) wnosimy, że P^2-5Q^2 nie jest podzielne ani przez 2, ani przez 5; musiałoby więc być $h\neq 2$ i $h\neq 5$, a ponieważ $h|2P$, więc byłoby $h|P$ i wobec tożsamości $5Q^2=P^2-(P^2-5Q^2)$ liczba pierwsza $h\neq 5$ byłaby dzielnikiem liczby $5Q^2$, skąd $h|Q$ wbrew (31). Tak więc okazaliśmy, że

$$([P+Q\sqrt{5}],[P-Q\sqrt{5}])=1. \tag{33}$$

Ponieważ każdy ideał ciała $K(\sqrt{5})$ może być przedstawiony w formie $[c+d\sqrt{5}]$, gdzie c i d są całkowite wymierne, więc na mocy (32) i (33) jest $[P+Q\sqrt{5}]=[c+d\sqrt{5}]^5$ skąd

$$P+Q\sqrt{5}=\varepsilon(c+d\sqrt{5})^5, \tag{34}$$

gdzie

$$|N(\varepsilon)|=1. \tag{35}$$

Niech

$$\varepsilon=u+v\omega,$$

gdzie u i v są całkowite wymierne. W myśl (35) jest

$$(P+Q\sqrt{5})(u+v\omega')=\pm(c+d\sqrt{5})^5=c_1+d_1\sqrt{5},$$

gdzie c_1 i d_1 są całkowite wymierne; zatem

$$(P+Q\sqrt{5})(2u+v-v\sqrt{5})=2c_1+2d_1\sqrt{5}$$

czyli $(2u+v)Q-vP=2d_1$, skąd wynika na mocy (27) i (29), że v jest parzyste. Możemy więc napisać

$$\varepsilon=u+v\frac{1+\sqrt{5}}{2}=\xi+\eta\sqrt{5};$$

zarazem wobec (35) $\xi^2-5\eta^2=\pm 1$.

Najmniejszym rozwiązaniem dodatnim tego równania jest układ 2, 1; wynika stąd na mocy twierdzenia 4 Rozdziału XI (§ 2, str. 259), uogólnionego na przypadek, gdy po prawej stronie równania Pella jest znak + lub — że przy pewnym n naturalnym oraz odpowiedniej kombinacji tych znaków jest

(36) $$\varepsilon=\xi+\eta\sqrt{5}=\pm(2\pm\sqrt{5})^n.$$

Niech

(37) $$(c+d\sqrt{5})^5=c_0+d_0\sqrt{5}.$$

W myśl (34) możemy więc napisać

(38) $$P+Q\sqrt{5}=\pm(2\pm\sqrt{5})^n(c_0+d_0\sqrt{5}).$$

Z (37) wynika, że liczby c_0 i d_0 są całkowite wymierne i że d_0 jest podzielne przez 5. Porównując po obu stronach (38) współczynniki przy $\sqrt{5}$, znajdujemy z łatwością $Q\equiv\pm n\,2^{n-1}c_0 \pmod 5$, a ponieważ w myśl (27) jest

(39) $$Q\equiv 0 \pmod 5,$$

więc

(40) $$n\,c_0\equiv 0 \pmod 5.$$

Podobnie, porównując w (38) części wymierne, znajdujemy

$$P\equiv\pm 2^n c_0 \pmod 5,$$

skąd wobec (30) $c_0\not\equiv 0 \pmod 5$, a więc na mocy (40) $n\equiv 0 \pmod 5$ czyli $n=5k$, gdzie k jest pewną liczbą naturalną. Na mocy (34) i (36) wynika stąd, że

$$P+Q\sqrt{5}=\{\pm(2\pm\sqrt{5})^k(c+d\sqrt{5})\}^5$$

czyli $P+Q\sqrt{5}=(s+t\sqrt{5})^5$, gdzie s i t są całkowite wymierne. Stosując równości (27), mamy zatem

(41) $$q^2+5^2r^2=s(s^4+2\cdot 5^2s^2t^2+5^3t^4),$$

(42) $$10r^2=5t(s^4+10s^2t^2+5t^4).$$

W myśl (17) musi więc być

(43) $$s>0, \qquad t>0,$$

a w myśl (27) i (31)

(44) $$(s,t)=1.$$

Ponieważ na mocy (27) i (29)

(45) $$s\not\equiv 0 \pmod 2,$$

więc musi być

(46) $$t\equiv 0 \pmod 2,$$

gdyż inaczej lewa strona równości (41) wypadłaby parzysta wbrew (27) i (29).

Ponieważ dalej na mocy (30), (27) i (41) jest

(47) $$s\not\equiv 0 \pmod 5,$$

więc musi być

(48) $$t\equiv 0 \pmod 5,$$

gdyż w przeciwnym razie prawa strona równości (42) byłaby w myśl (47) niepodzielna przez 25, gdy tymczasem lewa jej strona jest podzielna przez 25 wobec pierwszej z równości (26), z której wynika, że $r\equiv 0 \pmod{5^3}$, a zatem że $10r^2\equiv 0 \pmod{5^7}$.

Mnożąc (26) przez 5^2, otrzymujemy $2\cdot 5^2r=(5a)^5$, skąd $2^2\cdot 5^4r^2=(5a)^{10}$, a więc w myśl (42), przy oznaczeniu $n_1=4$,

(49) $$(5a)^{10}=2\cdot 5^{n_1}t(s^4+10s^2t^2+5t^4).$$

W równości tej ostatni czynnik prawej strony jest na mocy (45) i (46) — jak łatwo widzieć — nieparzysty, na mocy (47) — niepodzielny przez 5, a na mocy (44) — pierwszy względem t. Jest on więc pierwszy względem iloczynu $2\cdot 5^4t$, skąd wynika wobec (49), że

(50) $$2\cdot 5^{n_1}t=a_1^5, \qquad s^4+10s^2t^2+5t^4=b_1^5,$$

gdzie a_1 i b_1 są całkowite wymierne. Przyjmując oznaczenia

(51) $$P_1=s^2+5t^2, \qquad Q_1=2t^2,$$

możemy drugą z równości (50) napisać w postaci

$$P_1^2-5Q_1^2=b_1^5$$

oraz — jak łatwo widzieć — okazać analogicznie do (30), (31) i (39), że

$$P_1\not\equiv 0 \pmod 5, \qquad (P_1,Q_1)=1, \qquad Q_1\equiv 0 \pmod 5.$$

Jak wyżej, otrzymujemy stąd

$$P_1+Q_1\sqrt{5}=(s_1+t_1\sqrt{5})^5,$$

skąd w myśl oznaczeń (51)

(52) $$s^2+5t^2=s_1(s_1^4+2\cdot 5^2 s_1^2 t_1^2+5^3 t_1^4),$$

(53) $$2t^2=5t_1(s_1^4+10 s_1^2 t_1^2+5t_1^4),$$

a więc wobec (43)

(54) $$s_1>0, \qquad t_1>0$$

i wobec $(P_1, Q_1)=1$

(55) $$(s_1, t_1)=1.$$

Wzór (52) wskazuje na mocy (45) i (46), że s_1 jest nieparzyste, więc t_1 parzyste, a na mocy (47), że

$$s_1\not\equiv 0 \pmod 5,$$

skąd na mocy (48) i (53)

$$t_1\equiv 0 \pmod 5.$$

Wobec (50) jest $2^2\cdot 5^{2n_1}t^2=a_1^{10}$, a więc w myśl równości (53) przy oznaczeniu $n_2=2n_1+1$

$$2\cdot 5^{n_2}t_1(s_1^4+10 s_1^2 t_1^2+5t_1^4)=a_1^{10}.$$

Z tego wzoru na mocy dowiedzionych własności liczb s_1 i t_1 wyprowadzamy dalsze wnioski podobnie jak wyżej ze wzoru (49) itd.

Mamy przy tym na mocy (53) i (54) nierówność $2t^2>25t_1^5$, skąd

$$t_1<\sqrt[5]{2t^2/25}<t.$$

Rozumując dalej w ten sam sposób, otrzymalibyśmy więc ciąg nieskończony malejący liczb naturalnych $t_1>t_2>\ldots$, co niemożliwe. Przypadek 1° musimy zatem odrzucić.

2° z jest nieparzyste. Z liczb x i y jedna jest więc parzysta, a druga nieparzysta. Pisząc

(56) $$x+y=p, \qquad x-y=q,$$

mamy stąd

(57) $$2x=p+q, \qquad 2y=p-q,$$

(58) $$p\not\equiv 0 \pmod 2, \qquad q\not\equiv 0 \pmod 2,$$

skąd widzimy w jednej chwili, że

(59) $$(p,q)=1.$$

Wnosząc (57) do równania (10), dostajemy po łatwej redukcji

(60) $$p(p^4+10p^2q^2+5q^4)=2^4z^5.$$

Gdyby p było niepodzielne przez 5, to lewa, a więc i prawa strona tej równości byłaby niepodzielna przez 5 wbrew (11). Zatem

(61) $$p=5r,$$

gdzie r jest całkowite wymierne. Stąd wobec (59)

(62) $$q\not\equiv 0 \pmod 5.$$

Na mocy (11), (60) i (61)

(63) $$r(5^3r^4+2\cdot 5^2r^2q^2+q^4)=2^4 5^3 t^5,$$

a na mocy (59) i (61)

(64) $$(r,q)=1.$$

Zauważmy, że czynniki lewej strony równości (63) są względnie pierwsze. Istotnie, gdyby liczby

$$r \quad \text{i} \quad 5^3r^4+2\cdot 5^2r^2q^2+q^4$$

miały wspólny dzielnik pierwszy h, to byłby to zarazem dzielnik liczby q^4, a więc też liczby q, wbrew (64). Jest zatem

$$(r,\ 5^3r^4+2\cdot 5^2r^2q^2+q^4)=1.$$

Wnosimy stąd, z uwagi na to, że pierwszy czynnik lewej strony równości (63) jest wobec (58) i (61) nieparzysty, a drugi wobec (62) — niepodzielny przez 5, że

(65) $$r=5^3a^5,$$

(66) $$5^3r^4+2\cdot 5^2r^2q^2+q^4=2^4b^5.$$

Pisząc

(67) $$q^2+5^2r^2=2P, \qquad 10r^2=2Q,$$

możemy równość (66) przedstawić w postaci

(68) $$P^2-5Q^2=4b^5,$$

gdzie a i b są całkowite wymierne.

Według (58) $q^2+5^2r^2$ jest liczbą parzystą formy $4k+2$. Na mocy pierwszej z równości (67) liczba P jest więc całkowita i

(69) $$P\not\equiv 0 \pmod 2,$$

a na mocy tejże równości i (62)

(70) $$P\not\equiv 0 \pmod 5.$$

W myśl zaś drugiej z równości (67) liczba Q jest całkowita i

(71) $$Q\equiv 0 \pmod 5,$$

a na mocy (58) i (61)

(72) $$Q\not\equiv 0 \pmod 2.$$

Gdyby więc liczby P i Q miały wspólny dzielnik pierwszy h, to wobec (70) musiałoby być $h\neq 5$, a że według (67) jest

$$q^2=2P-5Q, \qquad 5r^2=Q,$$

więc liczba h byłaby wspólnym dzielnikiem liczb q i r wbrew (64). Zatem

(73) $$(P,Q)=1.$$

Wobec (68) możemy napisać

(74) $$\left[\frac{P+Q\sqrt{5}}{2}\right]\cdot\left[\frac{P-Q\sqrt{5}}{2}\right]=[b]^5,$$

a z (69) i (72) wynika bez trudności, że liczby

$$\frac{P+Q\sqrt{5}}{2} \quad \text{i} \quad \frac{P-Q\sqrt{5}}{2}$$

są całkowite w ciele $K(\sqrt{5})$.

Okażemy, że są one ideałami względnie pierwszymi. Istotnie, gdyby było

$$\left[\frac{P+Q\sqrt{5}}{2}\right]=[\lambda_1][\lambda_0], \qquad \left[\frac{P-Q\sqrt{5}}{2}\right]=[\lambda_2][\lambda_0],$$

gdzie λ_0, λ_1, λ_2 są liczbami całkowitymi ciała $K(\sqrt{5})$ i $[\lambda_0]\neq[1]$, to mielibyśmy

$$P+Q\sqrt{5}=2\varepsilon_1\lambda_1\lambda_0, \qquad P-Q\sqrt{5}=2\varepsilon_2\lambda_2\lambda_0,$$

skąd

$$P=(\varepsilon_1\lambda_1+\varepsilon_2\lambda_2)\lambda_0, \qquad P^2-5Q^2=4\varepsilon_1\varepsilon_2\lambda_1\lambda_2\lambda_0^2,$$

co dowodzi, że ideał $[\lambda_0]\neq[1]$ byłby wspólnym dzielnikiem ideałów $[P]$ i $[P^2-5Q^2]$. Zatem liczby P i P^2-5Q^2 nie mogłyby być względnie pierwsze w dziedzinie liczb wymiernych. Lecz każdy wspólny dzielnik pierwszy tych liczb, jako różny od 5 wobec (70), musiałby być zarazem dzielnikiem liczby Q wbrew (73). Dowiedliśmy więc, że

$$\left(\left[\frac{P+Q\sqrt{5}}{2}\right],\left[\frac{P-Q\sqrt{5}}{2}\right]\right)=1,$$

skąd wynika według (74), z uwagi na to, że każdy ideał ciała $K(\sqrt{5})$ może być przedstawiony w formie $[c+d\sqrt{5}]$, gdzie c i d są całkowite wymierne, że

$$\left[\frac{P+Q\sqrt{5}}{2}\right]=[c+d\sqrt{5}]^5,$$

a zatem

(75) $$\frac{P+Q\sqrt{5}}{2}=\varepsilon(c+d\sqrt{5})^5,$$

gdzie ε jest dzielnikiem jedności w ciele $K(\sqrt{5})$.

Lecz z twierdzenia 10 Rozdziału XVII (§ 6, str. 434) wynika, że każdy dzielnik jedności w ciele $K(\sqrt{5})$ ma postać

$$\varepsilon=\pm\left(\frac{1+\sqrt{5}}{2}\right)^n,$$

gdzie n jest liczbą całkowitą wymierną. Ponieważ oczywiście

$$\left(\frac{1+\sqrt{5}}{2}\right)^{-1}=-\frac{1-\sqrt{5}}{2},$$

więc możemy jeszcze napisać

$$\varepsilon=\pm\left(\frac{1\pm\sqrt{5}}{2}\right)^n,$$

gdzie n jest liczbą całkowitą wymierną nieujemną. Stąd według (75)

(76) $$\frac{P+Q\sqrt{5}}{2}=\pm\left(\frac{1\pm\sqrt{5}}{2}\right)^n\cdot(c+d\sqrt{5})^5,$$

a że $(c+d\sqrt{5})^5=c_1+d_1\sqrt{5}$, gdzie c_1 i d_1 są całkowite wymierne oraz $d_1\equiv 0 \pmod 5$, więc

$$2^{n-1}(P+Q\sqrt{5})=\pm(1\pm\sqrt{5})^n(c_1+d_1\sqrt{5}),$$

skąd

(77) $$2^{n-1}P\equiv\pm c_1 \pmod 5, \qquad 2^{n-1}Q\equiv\pm nc_1 \pmod 5,$$

przy czym znaki $+$ i $-$ w tych kongruencjach mogą nie być zgodne. Pierwsza z nich dowodzi wobec (70), że

(78) $$c_1 \not\equiv 0 \pmod 5,$$

skąd na mocy drugiej z nich i (71) jest $n \equiv 0 \pmod 5$ czyli $n = 5k$, gdzie k jest liczbą całkowitą wymierną nieujemną. Stąd według (76)

(79) $$\frac{P+Q\sqrt{5}}{2} = \pm\left(\frac{1\pm\sqrt{5}}{2}\right)^{5k}(c+d\sqrt{5})^5.$$

Udowodnimy teraz, że przy wszelkim całkowitym $k \geqslant 0$ jest

(80) $$\left(\frac{1\pm\sqrt{5}}{2}\right)^k = \frac{a+b\sqrt{5}}{2},$$

gdzie a i b są liczbami całkowitymi wymiernymi, z których obie są parzyste lub obie nieparzyste. Istotnie, równość (80) zachodzi dla $k=0$. Załóżmy, że zachodzi ona dla pewnego $k \geqslant 0$. Wynika z niej, że

(81) $$\left(\frac{1\pm\sqrt{5}}{2}\right)^{k+1} = \frac{a\pm 5b+(b\pm a)\sqrt{5}}{4},$$

a skoro a i b są jednocześnie parzyste lub nieparzyste, to

$$a \pm 5b = 2a_1 \quad \text{i} \quad b \pm a = 2b_1,$$

gdzie a_1 i b_1 są całkowite, skąd

$$a_1 \pm b_1 = a \pm 3b,$$

co dowodzi, że liczby a_1 i b_1 są również obie parzyste lub obie nieparzyste. Wobec (81) wnosimy więc, że równość (80) zachodzi dla $k+1$, a stąd przez indukcję, że zachodzi ona przy wszelkim całkowitym $k \geqslant 0$.

Na mocy (79) i (80) jest zatem

$$\frac{P+Q\sqrt{5}}{2} = \frac{[\pm(a+b\sqrt{5})(c+d\sqrt{5})]^5}{2^5}$$

czyli

$$P+Q\sqrt{5} = \frac{(s+t\sqrt{5})^5}{2^4},$$

gdzie s i t są liczbami całkowitymi wymiernymi. Stąd

(82) $$16P = s(s^4+2\cdot 5^2 s^2t^2+5^3t^4), \qquad 16Q = 5t(s^4+10s^2t^2+5t^4).$$

Z równości tych wynika według (73), że liczby s i t nie mają wspólnego dzielnika nieparzystego większego od 1. Gdyby obie liczby s i t były parzyste, to prawe strony równości (82) byłyby podzielne przez 32 wbrew (69). Jest więc

(83) $$(s,t)=1.$$

Pierwsza z równości (82) daje na mocy (70)

(84) $$s \not\equiv 0 \pmod 5.$$

Gdyby s było parzyste, a więc — w myśl (83) — t nieparzyste, to w drugiej z równości (82) prawa strona byłaby nieparzysta, co niemożliwe.

Gdyby zaś t było parzyste, a więc s nieparzyste, to znów w pierwszej z tych równości prawa strona byłaby nieparzysta, co też niemożliwe.

Jest więc

(85) $$s \not\equiv 0 \pmod 2,$$

jako też

(86) $$t \not\equiv 0 \pmod 2.$$

Na mocy (65) i (67) jest $Q = 5^7 a^{10}$, skąd wobec (82)

(87) $$t(s^4+10s^2t^2+5t^4) = 16\cdot 5^6\cdot(a^2)^5.$$

Na mocy (83), czynniki lewej strony są tu — jak łatwo widzieć — względnie pierwsze; przy tym pierwszy jest w myśl (86) nieparzysty, a drugi w myśl (84) — niepodzielny przez 5. Stąd wnosimy wobec (87), że

(88) $$t = 5^6 a_1^5$$

oraz $s^4+10s^2t^2+5t^4 = 16b_1^5$, co możemy w oznaczeniach

(89) $$s^2+5t^2 = 2P_1, \qquad t^2 = Q_1,$$

napisać też w postaci

(90) $$P_1^2 - 5Q_1^2 = 4b_1^5,$$

gdzie a_1 i b_1 są liczbami całkowitymi wymiernymi.

Równości (89) wskazują wobec (85) i (86), że liczby P_1 i Q_1 są całkowite nieparzyste, a wobec (83), że

$$(P_1, Q_1) = 1;$$

druga zaś z równości (89) daje na mocy (88)

$$Q_1 \equiv 0 \pmod 5.$$

Zarazem $r \neq 0$ na mocy (58) i (61), wobec czego drugie z równości (67) i (82) dają

$$t > 0.$$

Postępując dalej z równaniem (90) jak wyżej z równaniem (68), doszlibyśmy do wzorów

$$(91) \qquad \begin{aligned} 16P_1 &= s_1(s_1^4 + 2\cdot 5^2 s_1^2 t_1^2 + 5^3 t_1^4), \\ 16Q_1 &= 5t_1(s_1^4 + 10 s_1^2 t_1^2 + 5 t_1^4), \end{aligned}$$

gdzie znowu s_1 i t_1 są liczbami całkowitymi wymiernymi i $t_1 > 0$. Drugi z tych wzorów daje $16Q_1 > 25t_1^5$, skąd na mocy drugiego ze wzorów (89)

$$t_1 < \sqrt[5]{\frac{16}{25}t^2} < t.$$

Rozumując dalej w ten sam sposób, otrzymalibyśmy więc ciąg nieskończony malejący liczb naturalnych $t_1 > t_2 > \ldots$, co niemożliwe. Przypadek 2° nie może zatem również zachodzić.

Równanie (10) nie jest przeto rozwiązalne w liczbach całkowitych wymiernych różnych od zera, c. b. d. o.

§ 3. Twierdzenie Fermata dla potęgi $n = 7$. Udowodnimy obecnie

Twierdzenie 2. *Równanie*

$$(92) \qquad x^7 + y^7 + z^7 = 0$$

nie jest rozwiązalne w liczbach całkowitych wymiernych, różnych od zera.

Dowód [1]). Przypuśćmy, że równanie (92) jest spełnione przez liczby całkowite x, y, z różne od 0 i nie mające wspólnego dzielnika większego od 1.

Łatwo sprawdzić tożsamość

$$(x+y+z)^7 - (x^7+y^7+z^7) =$$
$$= 7(x+y)(y+z)(x+z)[(x^2+y^2+z^2+xy+yz+zx)^2 + xyz(x+y+z)].$$

[1]) Według V.-A. Lebesgue'a, Journal des Mathématiques 5 (1840), str. 276 i 348.

Tożsamość tę można wyprowadzić, wyrażając według znanych metod funkcję symetryczną $x^7+y^7+z^7$ przez funkcje $x+y+z$, $xy+yz+zx$ i xyz oraz zważywszy, że

$$(x+y)(y+z)(z+x) = (x+y+z)(xy+yz+zx) - xyz,$$
$$x^2+y^2+z^2+xy+yz+zx = (x+y+z)^2 - (xy+yz+zx).$$

Niech

$$(93) \qquad s = x+y+z,$$
$$(94) \qquad u = x^2+y^2+z^2+xy+yz+zx,$$
$$(95) \qquad v = (x+y)(y+z)(z+x),$$
$$(96) \qquad t = u^2 + xyzs.$$

Na mocy wspomnianej tożsamości i założenia, że liczby x, y i z spełniają równanie (92), jest

$$(97) \qquad s^7 = 7vt.$$

Jedna z liczb x, y, z jest parzysta, a dwie nieparzyste. Wobec (94) u jest więc nieparzyste, a wobec (93) s jest parzyste; ponieważ zaś $xyz \equiv 0 \pmod 2$, więc $xyzs \equiv 0 \pmod 4$, skąd mamy wobec (96)

$$(98) \qquad t \equiv u^2 \equiv 1 \pmod 4$$

czyli

$$(99) \qquad t = 4k+1$$

dla pewnego k naturalnego. Z (97) wynika dalej, że jeżeli h jest dzielnikiem pierwszym liczby t, to h jest też dzielnikiem liczby s, a zatem według (96) — również dzielnikiem liczby u.

Gdyby więc liczby t i x miały wspólny dzielnik pierwszy h, to byłby on też wspólnym dzielnikiem liczb s i u, a więc wobec (93) — także dzielnikiem liczby $y+z = s-x$ i wobec (94) — dzielnikiem liczby

$$y^2+z^2+yz = u - x(x+y+z).$$

Lecz

$$y^2+z^2+yz = (y+z)^2 - yz;$$

liczba h byłaby więc dzielnikiem liczby yz wbrew założeniu, że liczby x, y, z nie mają wspólnego dzielnika większego od 1.

Dowiedliśmy więc, że $(t, x) = 1$, i podobnie dowiedlibyśmy, że $(t, y) = 1$ oraz $(t, z) = 1$.

Tak więc

(100) $$(t, xyz) = 1.$$

Z (95) znajdujemy z łatwością

(101) $$v = s(xy + yz + zx) - xyz,$$

a ponieważ — jak widzieliśmy — każdy dzielnik pierwszy liczby t jest też dzielnikiem liczby s, więc równość (101) wskazuje, że gdyby v i t miały wspólny dzielnik pierwszy h, to byłby on zarazem dzielnikiem liczby xyz wbrew (100). Zatem

(102) $$(t, v) = 1.$$

Okażemy, że każda liczba pierwsza różna od 7, o ile jest dzielnikiem liczby t, wchodzi do rozkładu liczby t w potędze podzielnej przez 14.

Niech $h \neq 7$ będzie dzielnikiem pierwszym liczby t i niech h wchodzi z wykładnikiem α do rozkładu liczby t na czynniki pierwsze. Wobec (97) i (102) wnosimy stąd, że h wchodzi też do rozkładu liczby s^7 w potędze o wykładniku α, skąd wynika, że $\alpha = 7\beta$, gdzie β jest wykładnikiem potęgi, z którą h wchodzi do rozkładu liczby s. Według (100) jest tym bardziej $(h, xyz) = 1$, skąd widać, że h wchodzi do rozkładu liczby $xyzs$ w potędze o wykładniku β. W myśl (96)

(103) $$t - xyzs = u^2;$$

różnica ta jest więc podzielna przez h^β (gdyż $\alpha = 7\beta > \beta$, $h^\alpha | t$ i $h^\beta | xyzs$), lecz nie jest już podzielna przez $h^{\beta+1}$ (gdyż $\alpha \geqslant \beta + 1$, $h^{\beta+1} | t$, a $xyzs$ nie jest podzielne przez $h^{\beta+1}$). Czynnik h wchodzi więc w potędze o wykładniku β do rozkładu liczby u^2. Wnosimy stąd, że β jest liczbą parzystą, $\beta = 2\gamma$, czyli $\alpha = 7\beta = 14\gamma$.

Okażemy teraz, że t jest niepodzielne przez 7.

Przypuśćmy, że tak nie jest. Na mocy (96) i (97) liczba 7 byłaby więc zarazem dzielnikiem liczb s i u. Niech α, β i γ będą odpowiednio wykładnikami, z którymi 7 wchodzi do rozkładów liczb t, s i u. Według (97) i (102) jest $7\beta = \alpha + 1$, skąd $\beta > 0$ i $\alpha > \beta$; znajdujemy stąd jak wyżej na mocy (100), że różnica (103) zawiera czynnik 7 w potędze o wykładniku β, skąd $\beta = 2\gamma$ i przeto $\alpha = 7\beta - 1 = 14\gamma - 1$.

Jeżeli więc $t \equiv 0 \pmod 7$, to t zawiera wszystkie czynniki pierwsze różne od 7 w potędze podzielnej przez 14, czynnik zaś 7 w potędze $14\gamma - 1$; stąd wniosek, że w razie $t \equiv 0 \pmod 7$ liczba $7t$ byłaby czternastą potęgą.

Lecz $7t = a^{14} = (a^7)^2$ daje na mocy (99) $(a^7)^2 \equiv 7 \equiv -1 \pmod 4$, co niemożliwe.

Zatem t jest niepodzielne przez 7, a przeto wobec (97) i (102)

(104) $$t = q^{14}.$$

Ponieważ każdy czynnik pierwszy liczby t, wchodzący do t w potędze α, wchodzi do u — jak dowiedliśmy — w potędze $\gamma = \alpha/14$, więc na mocy (104) jest

(105) $$u = qr, \quad \text{gdzie} \quad (q, r) = 1,$$

i wobec nieparzystości liczby u liczby q i r są też nieparzyste.

Wobec $t \not\equiv 0 \pmod 7$ i (102) jest $(7v, t) = 1$, skąd wynika na mocy (97), że $7v = (7p)^7$ czyli

(106) $$v = 7^6 p^7,$$

a ponieważ dwie z liczb x, y, z są nieparzyste, więc wobec (95) v jest parzyste; zatem wobec (106) p też jest parzyste.

Na mocy (106) i (95), (104) i (96) oraz (93), (94) i (97) możemy przeto napisać

(a) $$(x + y)(y + z)(z + x) = 7^6 p^7,$$

(b) $$(x^2 + y^2 + z^2 + xy + yz + xz)^2 + (x + y + z)xyz = q^{14},$$

(c) $$x + y + z = 7pq^2$$

i wreszcie wobec (105)

(d) $$x^2 + y^2 + z^2 + xy + yz + zx = qr.$$

Równości (c) i (d) dają

$$xy + yz + zx = 7^2 p^2 q^4 - qr,$$

skąd mnożąc stronami przez (c) i biorąc pod uwagę (a), znajdujemy

$$xyz = 7pq^2(7^2 p^2 q^4 - qr) - 7^6 p^7,$$

wobec czego (b) daje w myśl (c) i (d)

$$q^{14} = q^2 r^2 + [7pq^2(7^2 p^2 q^4 - qr) - 7^6 p^7]\, 7pq^2.$$

Zatem

$$q^{12} = r^2 + 7^2 p^2 q^3 (7^2 p^2 q^3 - r) - 7^7 p^8,$$

co możemy też napisać w postaci

$$(r-{}^1/_2 7^2p^2q^3)^2=q^{12}-3({}^1/_2 7^2p^2q^3)+7^7p^3. \tag{107}$$

Gdyby było $p=0$, to mielibyśmy $v=0$ na mocy (106) i byłoby też $s=0$ na mocy (c), skąd $xyz=0$ na mocy (101), wbrew założeniu, że żadna z liczb x, y, z nie jest zerem.

Możemy więc przyjąć $p^2=2^{\alpha+1}r_1$, gdzie r_1 jest nieparzyste i gdzie $\alpha\geqslant 1$ wobec parzystości liczby p.

Niech

$$r-{}^1/_2 7^2p^2q^3=p_1, \qquad q^3=q_1. \tag{108}$$

Wobec parzystości liczby p i nieparzystości liczby r liczba p_1 jest więc całkowita. Liczba q_1 jest nieparzysta wobec nieparzystości liczby q. Wreszcie i liczba r_1 jest nieparzysta. Równość (107) przybiera zatem postać

$$p_1^2=q_1^4-2^{2\alpha}3\cdot 7^4q_1^2r_1^2+2^{4\alpha+4}\cdot 7^7r_1^4. \tag{109}$$

Według (102), (104) i (106) jest $(p,q)=1$; według (108) jest zatem $(r_1,q_1)=1$, ze (109) zaś wynika wobec nieparzystości liczby p_1, że każdy wspólny dzielnik pierwszy liczb p_1 i r_1 byłby też dzielnikiem liczby q_1, a każdy wspólny dzielnik pierwszy liczb p_1 i q_1, który musi być różny od 7, gdyż $q_1|q$ i $q|t$, byłby też dzielnikiem liczby r_1. Jest więc

$$(r_1,q_1)=1, \qquad (r_1,p_1)=1, \qquad (p_1,q_1)=1. \tag{110}$$

Równość (109) możemy napisać w postaci

$$\begin{aligned}[p_1+(q_1^2-2^{2\alpha-1}3\cdot 7^4r_1^2)]\,[p_1-(q_1^2-2^{2\alpha-1}3\cdot 7^4r_1^2)]&=\\ =2^{4\alpha-2}7^7r_1^4.&\end{aligned} \tag{111}$$

Niech

$$p_1+q_1^2-2^{2\alpha-1}3\cdot 7^4r_1^2=P, \qquad p_1-q_1^2+2^{2\alpha-1}3\cdot 7^4r_1^2=Q. \tag{112}$$

Gdyby jednocześnie było

$$P\equiv 0 \pmod 7, \qquad Q\equiv 0 \pmod 7,$$

to byłoby też w myśl (112)

$$p_1+q_1^2\equiv 0 \pmod 7, \qquad p_1-q_1^2\equiv 0 \pmod 7,$$

skąd wynikałoby wbrew (110), że liczby $2p_1$ i $2q_1^2$ są podzielne przez 7.

Zupełnie tak samo dowiedlibyśmy, że liczby P i Q nie mają wspólnego dzielnika pierwszego h, będącego dzielnikiem liczby r_1, gdyż taki dzielnik musiałby być nieparzysty i mielibyśmy

$$p_1+q_1^2\equiv (\text{mod } h), \qquad p_1-q_1^2\equiv 0 \pmod h,$$

skąd $2p_1\equiv 2q_1^2\equiv 0 \pmod h$ i $p_1\equiv q_1\equiv 0 \pmod h$ wbrew (110).

Z (111) i (112) wynika równość

$$PQ=2^{4\alpha-2}7^7r_1^4, \tag{113}$$

z której wnosimy, że jedna z liczb P i Q jest podzielna, a druga niepodzielna przez 7; jeżeli zaś h jest jakimkolwiek dzielnikiem pierwszym liczby r_1, to jedna z liczb P i Q jest podzielna, a druga niepodzielna przez h.

Wobec (112) oraz nieparzystości liczb p_1 i q_1 jest

$$P\equiv Q\equiv 0 \pmod 2.$$

Gdyby było $\alpha=1$, to z uwagi na nieparzystość liczb q_1 i r_1 mielibyśmy wobec (109)

$$p_1^2\equiv q_1^4-4\cdot 3(7^2q_1r_1)^2\equiv q_1^4-4\cdot 3 \pmod 8,$$

skąd

$$p_1^2\equiv (q_1^2)+4 \pmod 8,$$

gdy tymczasem różnica dwu kwadratów nieparzystych jest podzielna przez 8.

Jest więc $\alpha>1$ czyli $\alpha\geqslant 2$, a zatem wobec (112)

$$p_1+q_1^2\equiv P \pmod 4, \qquad p_1-q_1^2\equiv Q \pmod 4,$$

co dowodzi, że nie może być $P\equiv Q\equiv 0 \pmod 4$, gdyż byłoby wtedy $2p_1\equiv 0 \pmod 4$, gdy tymczasem p_1 jest nieparzyste.

Z liczb P i Q jedna więc zawiera w swym rozwinięciu czynnik 2 w potędze 1, a druga w potędze $4\alpha-3$. Rozróżnimy dalej cztery następujące przypadki:

1° P nie jest podzielne ani przez 4, ani przez 7.
2° P nie jest podzielne przez 4, lecz jest podzielne przez 7.
3° P jest podzielne przez 4, lecz nie jest podzielne przez 7.
4° P jest podzielne i przez 4, i przez 7.

W przypadku 2^0, wobec udowodnionych własności liczb P i Q oraz z uwagi na to, że żaden dzielnik pierwszy liczby r_1 nie jest wspólnym dzielnikiem liczb P i Q, otrzymujemy w jednej chwili według (113)

$$P=2\cdot 7^7 a_1^4, \qquad Q=2^{4\alpha-3} b_1^4,$$

gdzie a_1 i b_1 są liczbami całkowitymi względnie pierwszymi. Stąd $P-Q=2(7^7 a_1^4-2^{4\alpha-4} b_1^4)$, a zatem w myśl (112)

$$q_1^2-2^{2\alpha-1}3\cdot 7^4 r_1^2=7^7 a_1^4-2^{4\alpha-4} b_1^4$$

i przeto wobec $\alpha>1$ oraz wobec nieparzystości liczby a_1 jako dzielnika liczby r_1

$$q_1^2\equiv 7^7 a_1^4\equiv 3 \pmod 4,$$

co niemożliwe.

W przypadku 4^0 znajdujemy podobnie

$$P=2^{4\alpha-3}7^7 a_1^4, \qquad Q=2b_1^4,$$

skąd $P-Q=2(2^{4\alpha-4}7^7 a_1^4-b_1^4)$ oraz w myśl (112)

$$q_1^2-2^{2\alpha-1}3\cdot 7^4 r_1^2=2^{4\alpha-4}7^7 a_1^4-b_1^4,$$

skąd wobec nieparzystości liczby b_1

$$q_1^2\equiv -b_1^4\equiv -1 \pmod 4,$$

co znowu niemożliwe.

W przypadku 3^0 znajdujemy

(114) $$P=2^{4\alpha-3}a_1^4, \qquad Q=2\cdot 7^7 b_1^4,$$

skąd $P-Q=2^{4\alpha-3}a_1^4-2\cdot 7^7 b_1^4$ oraz w myśl (112)

(115) $$q_1^2-2^{2\alpha-1}3\cdot 7^4 r_1^2=2^{4\alpha-4}a_1^4-7^7 b_1^4,$$

co wobec $r_1=a_1 b_1$ możemy też napisać w postaci

$$(2^{2\alpha-2}a_1^2+3\cdot 7^4 b_1^2)^2-q_1^2=2^6 7^7 b_1^4$$

czyli

(116) $$(2^{2\alpha-2}a_1^2+3\cdot 7^4 b_1^2+q_1)(2^{2\alpha-2}a_1^2+3\cdot 7^4 b_1^2-q_1)=2^6 7^7 b_1^4.$$

Wobec nieparzystości liczb b_1 i q_1 oba czynniki po stronie lewej są parzyste, ale nie mogą być oba podzielne przez 4, gdyż

ich różnica $2q_1$ jest niepodzielna przez 4. Podobnie, nie mogą one być oba podzielne przez 7, gdyż wtedy liczba $2q_1$, a więc i liczba q_1, byłaby podzielna przez 7, zatem wobec (115) liczba a_1 też byłaby podzielna przez 7 i byłoby $(q_1, a_1)\geqslant 7$, gdy tymczasem $a_1 | r_1$ i $(q_1, r_1)=1$.

Oznaczmy przez

$$2^{2\alpha-2}a_1^2+3\cdot 7^4 b_1^2\pm q_1$$

ten z czynników lewej strony równości (116), który nie jest podzielny przez 4.

Gdyby jakiś dzielnik pierwszy h liczby b_1 był wspólnym dzielnikiem obu czynników lewej strony równości (116), to ich suma $2^{2\alpha-1}a_1^2+2\cdot 3\cdot 7^4 b_1^2$ byłaby podzielna przez h, a zatem wobec $h | b_1$ i wobec nieparzystości liczby h byłoby $h | a_1$ czyli $(a_1, b_1)\geqslant h$, gdy tymczasem $(a_1, b_1)=1$.

Tak więc w razie, gdy czynnik lewej strony równości (116), niepodzielny przez 4, jest zarazem niepodzielny przez 7, mamy:

(117) $$\begin{aligned} 2^{2\alpha-2}a_1^2+3\cdot 7^4 b_1^2\pm q_1&=2c_1^4,\\ 2^{2\alpha-2}a_1^2+3\cdot 7^4 b_1^2\mp q_1&=2^5\cdot 7^7 d_1^4,\end{aligned}$$

w przeciwnym zaś razie:

(118) $$\begin{aligned} 2^{2\alpha-2}a_1^2+3\cdot 7^4 b_1^2\pm q_1&=2\cdot 7^7 c_1^4,\\ 2^{2\alpha-2}a_1^2+3\cdot 7^4 b_1^2\mp q_1&=2^5 d_1^4,\end{aligned}$$

gdzie c_1 i d_1 są liczbami całkowitymi oraz c_1 jest nieparzyste.

Równości (117) dają

$$2^{2\alpha-2}a_1^2=c_1^4-3\cdot 7^4 b_1^2+2^4\cdot 7^7 d_1^4,$$

co niemożliwe, gdyż lewa strona jest kwadratem, a prawa, wobec nieparzystości liczb c_1 i b_1, przystaje do $1-3=2$ modulo 4.

Równości zaś (118) dają

$$2^{2\alpha-2}a_1^2=7^7 c_1^4-3\cdot 7^4 b_1^2+2^4 d_1^4$$

lub, ponieważ $b_1=c_1 d_1$,

$$2^{2\alpha-2}a_1^2=7^7 c_1^4-3\cdot 7^4 c_1^2 d_1^2+2^4 d_1^4.$$

Mnożąc obie strony przez 2^6, dostajemy

$$2^{2\alpha+4}a_1^2-(2^5d_1^2-3\cdot 7^4c_1^2)^2=7^7c_1^4,$$

skąd

$$(2^{\alpha+2}a_1+2^5d_1^2-3\cdot 7^4c_1^2)(2^{\alpha+2}a_1-2^5d_1^2+3\cdot 7^4c_1^2)=7^7c_1^4.$$

Suma czynników po lewej stronie wynosi $2^{\alpha+3}a_1$, jest więc pierwsza względem c_1 wobec $(a_1,b_1)=1$, $b_1=c_1d_1$ i nieparzystości liczby b_1. Zarazem jest ona niepodzielna przez 7 wobec (114) i na mocy założeń rozważanego przypadku 3°. Czynniki lewej strony są więc względnie pierwsze. Mamy zatem przy odpowiednim znaku:

$$2^{\alpha+2}a_1\pm(2^5d_1^2-3\cdot 7^4c_1^2)=m^4,\qquad 2^{\alpha+2}a_1\mp(2^5d_1^2-3\cdot 7^4c_1^2)=7^7n^4,$$

skąd

$$2^{\alpha+3}a_1=m^4+7^7n^4. \tag{119}$$

Lecz liczby m i n są nieparzyste, ponieważ $mn=c_1$, $c_1\mid b_1$, $b_1\mid r_1$ i r_1 jest nieparzyste. Zatem $m^4\equiv n^4\equiv 1 \pmod{16}$, skąd

$$7^7n^4\equiv 7^7\equiv 7\cdot 49^3\equiv 7(3\cdot 16+1)^3\equiv 7 \pmod{16},$$

czyli prawa strona równości (119) przystawałaby do $1+7=8$ modulo 16, gdy tymczasem lewa strona tej równości jest podzielna przez $2^{\alpha+3}$, gdzie $\alpha>0$.

Dowiedliśmy więc, że również przypadek 3° jest niemożliwy.

Pozostaje przypadek 1°. Wobec założeń, które teraz mamy dla liczb P i Q, jest na mocy (113):

$$P=2a_1^4,\qquad Q=2^{4\alpha-3}\cdot 7^7b_1^4,\qquad (a_1b_1=r_1), \tag{120}$$

skąd

$$P-Q=2(a_1^4-2^{4\alpha-4}7^7b_1^4),$$

czyli w myśl (112)

$$q_1^2-2^{2\alpha-1}3\cdot 7^4a_1^2b_1^2=a_1^4-2^{4\alpha-4}7^7b_1^4,$$

a więc

$$(a_1^2+2^{2\alpha-2}3\cdot 7^4b_1^2+q_1)(a_1^2+2^{2\alpha-2}3\cdot 7^4b_1^2-q_1)=$$
$$=2^{4\alpha+2}7^7b_1^4. \tag{121}$$

Różnica czynników po lewej stronie wynosi $2q_1$; oba one są parzyste wobec nieparzystości liczb q_1 i a_1 (gdyż $a_1\mid r_1$), lecz

jeden tylko jest podzielny przez 4. Wobec $(q_1,r_1)=1$ jest więc tym bardziej $(q_1,b_1)=1$, skąd widać, że żaden dzielnik pierwszy liczby b_1 nie jest wspólnym dzielnikiem czynników lewej strony równości (121).

W rozważanym przypadku 1° liczba a_1 jest wobec (120) niepodzielna przez 7 i przeto suma czynników po lewej stronie równości (121) jest niepodzielna przez 7. Wynika stąd, że jeden tylko z tych czynników jest podzielny przez 7. Mamy więc przy stosownym znaku, w razie gdy czynnik podzielny przez 4 jest zarazem podzielny przez 7:

$$\begin{aligned} a_1^2+2^{2\alpha-2}3\cdot 7^4b_1^2\pm q_1&=2c_1^4,\\ a_1^2+2^{2\alpha-2}3\cdot 7^4b_1^2\mp q_1&=2^{4\alpha+1}7^7d_1^4, \end{aligned} \tag{122}$$

w przeciwnym zaś razie:

$$\begin{aligned} a_1^2+2^{2\alpha-2}3\cdot 7^4b_1^2\pm q_1&=2\cdot 7^7c_1^4,\\ a_1^2+2^{2\alpha-2}3\cdot 7^4b_1^2\mp q_1&=2^{4\alpha+1}d_1^4. \end{aligned} \tag{123}$$

Równości (123) dają

$$a_1^2+2^{2\alpha-2}3\cdot 7^4b_1^2=7^7c_1^4+2^{4\alpha}d_1^4,$$

gdzie prawa strona przystaje do

$$7^7c_1^4\equiv 3 \pmod 4,$$

gdy tymczasem lewa strona przystaje wobec $\alpha>1$ do

$$a_1^2 \pmod 4.$$

Równości (123) zachodzić więc nie mogą. Pozostają przeto edynie równości (122), które dają wobec $b_1=c_1d_1$ równość

$$a_1^2=c_1^4-2^{2(\alpha-1)}3\cdot 7^4c_1^2d_1^2+2^{4(\alpha-1)+4}7^7d_1^4, \tag{124}$$

różniącą się od (109) tylko tym, że liczby p_1, q_1, r_1 i α są zastąpione przez a_1, c_1, d_1 i $\alpha-1$, przy czym znowu liczby a_1, c_1, d_1 są nieparzyste oraz

$$(a_1,c_1)=1,\qquad (a_1,d_1)=1,\qquad (c_1,d_1)=1.$$

Jeżeli $\alpha - 1 > 1$, to postępując z równaniem (124) podobnie jak z równaniem (109), dochodzimy do równości

$$a_2^2 = c_2^4 - 2^{2(\alpha-2)} 3 \cdot 7^4 c_2^2 d_2^2 + 2^{4(\alpha-2)+4} 7^7 d_2^4$$

itd. aż wreszcie dojdziemy do równości

$$a_0^2 = c_0^4 - 2^2 3 \cdot 7^4 c_0^2 d_0^2 + 2^8 7^7 d_0^4,$$

która jest niemożliwa, gdyż liczby a_0, c_0 i d_0 są nieparzyste, lewa więc strona jest formy $8k+1$, a prawa formy $8k+5$.

Równanie (92) nie jest więc rozwiązalne w liczbach całkowitych wymiernych różnych od zera, c. b. d. o.

Nierozwiązalność równania $x^n + y^n = z^n$ w liczbach naturalnych dla $n=6$ i dla $n=9$ wynika z jego nierozwiązalności dla $n=3$, udowodnionej w Rozdziale XVII, § 9 (gdyż zarówno szósta jak i dziewiąta potęga liczby całkowitej jest sześcianem liczby całkowitej). Podobnie, nierozwiązalność tego równania dla $n=8$ i dla $n=10$ wynika z udowodnionej jego nierozwiązalności dla $n=4$ i $n=5$.

Dowiedliśmy więc wielkiego twierdzenia Fermata dla wszystkich wykładników n od 3 do 10 włącznie.

Zauważmy na zakończenie, że dla liczb pozaskończonych wielkie twierdzenie Fermata jest fałszywe: trójka $x=\omega+1$, $y=\omega$ i $z=\omega\cdot 2$ daje równość $(\omega+1)^n+\omega^n=(\omega\cdot 2)^n$ dla wszystkich n naturalnych.