Teoria liczb
zadania różne, 27 lutego

Uwaga ogólna: w rozwiązaniach poniżej preferujemy obliczenia "na palcach" tam, gdzie są one sensowne. Ponadto, rozwiązanie te są tak naprawdę szkicami. Niestety mogą zdarzyć się literówki, w razie znalezienia istotnych błędów, bardzo proszę o informację.

Zadanie 1. Nieparzysta liczba pierwsza p zapisuje się jako $a^2 + b^2$ dla pewnych całkowitych a, b. Pokaż, że $p \equiv 1 \pmod 4$.

Rozwiązanie.

Sprawdzając wszystkie reszty, dochodzimy do wniosku, że dla każdego a całkowitego mamy $a^2 \equiv 0 \pmod 4$ lub $a^2 \equiv 1 \pmod 4$. Wynika stąd, że $p = a^2 + b^2$ daje resztę $0 = 0 + 0$, $1 = 1 + 0$ lub $2 = 1 + 1$ z dzielenia przez cztery. Liczba p jest nieparzysta, zatem jedyna możliwość to reszta 1. (W rozwiązaniu nie używamy faktu, że p jest pierwsza.)

Zadanie 2. Pokaż, że równanie $x^3 + 2y^3 = 7^n$ nie ma rozwiązań w liczbach całkowitych dodatnich x, y, n.

Rozwiązanie.

Sprawdzając wszystkie możliwe reszty, dochodzimy do wniosku, że dla każdego a całkowitego a^3 daje resztę 0, 1 lub -1. Zatem $x^3 + 2y^3$ daje jedną z reszt $0 + 0$, $0 + 2$, $0 - 2$, $1 + 0$, $1 + 2$, $1 - 2$, $-1 + 0$, $-1 + 2$, $-1 - 2$. Reszta 0 jest możliwa tylko jako suma $0 + 0$, innymi słowy, $x^3 + 2y^3$ *jest podzielna przez* 7 *wtedy i tylko wtedy, gdy* x *oraz* y *są podzielne przez* 7.

Załóżmy, że istnieje rozwiązanie równania i wybierzmy takie rozwiązanie, dla którego n jest minimalne. Skoro x, y są dodatnie, to $x^3 + 2y^3 > 1$, zatem $n \geq 1$ i $x^3 + 2y^3 \equiv 0 \pmod 7$. Z uwagi na początku rozwiązania mamy, że 7 dzieli x oraz y. Zatem $x = 7x'$, $y = 7y'$. Wynika stąd, że

$$(x')^3 + 2(y')^3 = \frac{1}{7^3}\left(x^3 + 2y^3\right) = 7^{n-3}$$

jest także rozwiązaniem naszego równania. Ponadto w tym nowym rozwiązaniu wykładnik "n" jest niższy niż w oryginalnym rozwiązaniu. Ale wybraliśmy n minimalne, zatem sprzeczność. Równanie nie ma rozwiązań w liczbach całkowitych dodatnich.

Zadanie 3. Liczba całkowita a jest względnie pierwsza z 105. Pokaż, że $a^{12} \equiv 1 \pmod{105}$. Ile jest liczb względnie pierwszych z 105 w zbiorze $\{0, 1, 2, \ldots, 105 - 1\}$?

Rozwiązanie.

Liczby 3, 5 i 7 są parami względnie pierwsze i mnożą się do 105. Zauważmy, że dla każdego a poniższe warunki są równoważne

- $a^{12} \equiv 1 \pmod{105}$,

- $105 \mid a^{12} - 1$,
- $3 \mid a^{12} - 1$ oraz $5 \mid a^{12} - 1$ oraz $7 \mid a^{12} - 1$,
- $a^{12} \equiv 1 \pmod 3$ oraz $a^{12} \equiv 1 \pmod 5$ oraz $a^{12} \equiv 1 \pmod 7$.

Sprawdzimy, że ostatni z tych równoważnych warunków zachodzi. Można to zrobić "na palcach" ale można też użyć małego twierdzenia Fermata:

(a) Skoro $\mathrm{NWD}(a, 105) = 1$, to 7 nie dzieli a, zatem $a^{7-1} \equiv 1 \pmod 7$. Podnosząc do kwadratu, otrzymujemy $a^{12} \equiv 1 \pmod 7$.

(b) Skoro $\mathrm{NWD}(a, 105) = 1$, to 5 nie dzieli a, zatem $a^{5-1} \equiv 1 \pmod 5$. Podnosząc do sześcianu, otrzymujemy $a^{12} \equiv 1 \pmod 5$.

(c) Skoro $\mathrm{NWD}(a, 105) = 1$, to 3 nie dzieli a, zatem $a^{3-1} \equiv 1 \pmod 3$. Podnosząc do szóstej potęgi, otrzymujemy $a^{12} \equiv 1 \pmod 3$.

Z wykładu 2.03 wynika, że $\mathbb{Z}_{105}^* \simeq \mathbb{Z}_3^* \times \mathbb{Z}_5^* \times \mathbb{Z}_7^*$, a stąd

$$|\mathbb{Z}_{105}^*| = |\mathbb{Z}_3^*| \cdot |\mathbb{Z}_5^*| \cdot |\mathbb{Z}_7^*| = (3-1)(5-1)(7-1) = 48.$$

Zadanie 4. Pokaż, że istnieje nieskończenie wiele liczb pierwszych p takich, że $p \equiv 3 \pmod 4$. Czy umiesz "elementarnie" pokazać to samo dla $p \equiv 1 \pmod 4$?

Rozwiązanie.

Załóżmy, że tych liczb jest skończenie wiele i niech A oznacza ich iloczyn. Liczba A jest nieparzysta, więc liczba $2A$ daje resztę dwa z dzielenia przez 4, zatem $2A + 1 \equiv 3 \pmod 4$.

Zapiszmy rozkład na czynniki pierwsze $2A+1 = p_1^{a_1} \dots p_k^{a_k}$. Liczby $p_1, \dots, p_k$ są nieparzyste. Gdyby wszystkie te liczby dawały resztę 1 z dzielenia przez cztery, to

$$2A + 1 = p_1^{a_1} \dots p_k^{a_k} \equiv 1^{a_1} \dots 1^{a_k} = 1 \pmod 4,$$

sprzeczność. Zatem istnieje choć jedna liczba p_i która nie daje reszty jeden z dzielenia przez 4. Skoro p_i jest nieparzysta, to jedyna możliwość to $p_i \equiv 3 \pmod 4$. Ale wtedy z założenia p_i dzieli A, więc $0 \equiv 2A + 1 \equiv 1 \pmod{p_i}$, sprzeczność. Ostatecznie sprzeczność dowodzi, że liczb pierwszych p takich, że $p \equiv 3 \pmod 4$ jest nieskończenie wiele. (Autor nie zna "elementarnego" dowodu dla $p \equiv 1 \pmod 4$. Pokażemy ten fakt jako szczególny przypadek twierdzenia Dirichleta.)

Zadanie 5 (istnienie generatora)**.** Niech p będzie nieparzystą liczbą pierwszą. W tym zadaniu pokażemy, że grupa multiplikatywna $\mathbb{Z}_p^* = \{1 \mod p, 2 \mod p, \dots, p-1 \mod p\}$ jest cykliczna rzędu $p - 1$.

(a) Niech $a, b \in \mathbb{Z}_p^*$ będą elementami rzędu r_1, r_2. Pokaż, że istnieją liczby całkowite dodatnie k, l takie, że rząd $a^k b^l$ to $\mathrm{NWW}(r_1, r_2)$.

(b) Niech r będzie największym rzędem elementu w $\mathbb{Z}_p^*$. Pokaż, że każdy element tej grupy ma rząd będący dzielnikiem r.

(c) Pokaż, że dla każdego d, równanie $x^d - 1 \equiv 0 \pmod{p}$ ma najwyżej d rozwiązań w $\mathbb{Z}_p$. Wykorzystaj fakt, że jest to ciało. Wywnioskuj, że r powyżej jest równe $p-1$.

Rozwiązanie.

W rozwiązaniu będziemy wielokrotnie korzystać z następującej obserwacji (Algebra I): jeśli rząd elementu g to $\mu \in \mathbb{Z}_+$, to dla każdej liczby naturalnej n zachodzi równoważność

$$(g^n \equiv 1 \pmod{p}) \iff n \equiv 0 \pmod{\mu}.$$

Wynika z niej, że dla każdego k rząd elementu g^k to $\mu/\operatorname{NWD}(\mu, k)$. Zaiste, z uwagi powyżej, dla każdego n mamy $(g^k)^n \equiv 1 \pmod{p}$ wtedy i tylko wtedy, gdy $kn \equiv 0 \pmod{\mu}$, czyli gdy μ dzieli kn. Najmniejszą liczbą dodatnią spełniającą tę podzielność jest właśnie $\mu/\operatorname{NWD}(\mu, k)$. (Ten wniosek też był na Algebrze I.)

Przejdźmy do rozwiązania.

(a) Załóżmy najpierw, że $\operatorname{NWD}(r_1, r_2) = 1$. Pokażemy, że w tym przypadku $k = l = 1$ spełnia warunek zadania. Niech ν będzie rzędem elementu ab. Mamy $(ab)^\nu \equiv 1 \pmod{p}$. Podnieśmy tę równość do potęgi r_1. Otrzymujemy

$$1 \equiv (ab)^{\nu \cdot r_1} = (a^{r_1})^\nu \cdot b^{\nu \cdot r_1} \equiv 1^\nu \cdot b^{\nu \cdot r_1} \pmod{p}.$$

Z uwagi na początku rozwiązania wynika, że r_2 dzieli liczbę $\nu \cdot r_1$. Ale $\operatorname{NWD}(r_1, r_2) = 1$, więc to znaczy, że r_2 dzieli ν. Podnosząc wyjściową równość do potęgi r_2 otrzymujemy podobnie, że r_2 dzieli ν. Zatem ν jest wielokrotnością $\operatorname{NWW}(r_1, r_2) = r_1 r_2$. Ponadto $(ab)^{r_1 r_2} \equiv 1 \pmod{p}$, więc $\nu = r_1 r_2$.

Przejdźmy teraz do ogólnego przypadku, tzn. bez założenia o $\operatorname{NWD}(r_1, r_2) = 1$. Zapiszmy $r_1 = p_1^{a_1} \dots p_n^{a_n}$, $r_2 = p_1^{b_1} \dots p_n^{b_n}$, gdzie p_i są różnymi liczbami pierwszymi. Zmieniając kolejność p_i, możemy założyć, że $a_1 \geq b_1$, $a_2 \geq b_2$, …, $a_s \geq b_s$ oraz $a_{s+1} < b_{s+1}$, …, $a_n < b_n$, dla pewnego s.

Weźmy $k = p_{s+1}^{a_{s+1}} \dots p_n^{a_n}$ oraz $l = p_1^{b_1} \dots p_s^{b_s}$. Na mocy uwagi wniosku z początku rozwiązania, rząd elementu a^k to $p_1^{a_1} \dots p_s^{a_s}$, zaś rząd elementu b^l to $p_{s+1}^{b_{s+1}} \dots p_n^{b_n}$. Rzędy te są względnie pierwsze, więc argumentując jak powyżej "dla $a = a^k, b = b^l$" otrzymujemy, że rząd $a^k b^l$ to $p_1^{a_1} \dots p_s^{a_s} p_{s+1}^{b_{s+1}} \dots p_n^{b_n} = \operatorname{NWW}(r_1, r_2)$, czyli tezę.

(b) Załóżmy, że jakiś inny element ma rząd s niebędący dzielnikiem r. Wtedy na mocy podpunktu (a) istnieje element o rzędzie $\operatorname{NWW}(r, s) > r$, sprzeczność z wyborem r.

(c) Skoro $\mathbb{Z}_p$ jest ciałem to istnieje co najwyżej d rozwiązań równania $x^d \equiv 1 \pmod{p}$ na mocy twierdzenia Bezóut. Na mocy podpunktu (b), każdy z $p-1$ elementów $\mathbb{Z}_p^*$ spełnia równanie $x^r \equiv 1 \pmod{p}$. Zatem $r \geq p-1$. Z małego twierdzenia Fermata wynika, że $r \leq p-1$, więc ostatecznie $r = p-1$. Dowolny element o rzędzie r jest generatorem.

Zadanie 6 (Twierdzenie Wilsona). (a) Niech p będzie liczbą pierwszą. Pokaż, że $(p-1)! \equiv -1 \pmod{p}$.

(b) Niech n będzie dowolną liczbą naturalną. Jakie reszty z dzielenia przez n może dać $(n-1)!$?

Rozwiązanie.

Niech $g \mod p$ będzie generatorem grupy cyklicznej $\mathbb{Z}_p^*$; istnienie generatora wynika z zadania 5. Wtedy mamy równość zbiorów

$$\{1 \mod p, 2 \mod p, \ldots, p-1 \mod p\} = \left\{g \mod p, g^2 \mod p, \ldots, g^{p-1} \mod p\right\},$$

więc

$$(p-1)! = 1 \cdot 2 \cdot \ldots \cdot (p-1) \equiv g^1 \cdot g^2 \cdot \ldots \cdot g^{p-1} = g^{\frac{p(p-1)}{2}} \pmod{p}.$$

Przypadek $p = 2$ jest jasny, załóżmy więc $p > 2$. Wtedy $p-1$ nie dzieli $p(p-1)/2$, więc na mocy uwagi o rzędzie z zadania 5 mamy

$$g^{\frac{p(p-1)}{2}} \not\equiv 1 \pmod{p}.$$

Ponadto

$$\left(g^{\frac{p(p-1)}{2}}\right)^2 = g^{p(p-1)} = (g^{p-1})^p \equiv 1^p = 1 \pmod{p}.$$

Oznaczmy dla jasności $G := g^{\frac{p(p-1)}{2}} \mod p$. Wtedy $G \not\equiv 1 \pmod{p}$ oraz $G^2 \equiv 1 \pmod{p}$. Z tej ostatniej kongruencji wynika, że p dzieli liczbę $G^2 - 1 = (G-1)(G+1)$. To znaczy, że p dzieli $G-1$ lub $G+1$, czyli $G \equiv 1 \pmod{p}$ lub $G \equiv -1 \pmod{p}$. Pierwszy przypadek jest wykluczony, zatem $G \equiv -1 \pmod{p}$, co kończy dowód dla przypadku liczby pierwszej p.

Załóżmy teraz, że n jest liczbą naturalną niepierwszą. Niech $1 < d < n$ będzie dzielnikiem n. Jeśli $d \neq n/d$, to w iloczynie $(n-1)!$ występują zarówno d jak i n/d, więc $(n-1)! \equiv 0 \pmod{n}$. Pozostaje rozważyć przypadek, gdy dla *dowolnego* dzielnika d mamy $d = n/d$, czyli $n = d^2$. Ta równość implikuje, że n ma *tylko jeden* nietrywialny dzielnik, więc $n = p^2$ dla pewnej liczby pierwszej p. Jeśli $p > 2$, to p oraz $2p$ występują w iloczynie $(n-1)!$, zatem znowu $(n-1)! \equiv 0 \pmod{n}$. Jeśli zaś $p = 2$, to $n = 4$ i wtedy

$$(n-1)! = 3! \equiv 2 \pmod{4},$$

Odpowiedź: $(n-1)! \mod n$ *jest równe* $-1 \mod n$, *jeśli* n *jest pierwsza*, $0 \mod n$ *jeśli* n *jest złożona i* $n \neq 4$ *oraz* $2 \mod n$, *jeśli* $n = 4$.

Zadanie 7. Niech p będzie nieparzystą liczbą pierwszą, zaś r będzie liczbą całkowitą niepodzielną przez r. Pokaż, że równanie $a^2 \equiv r \pmod{p}$ ma rozwiązanie wtedy i tylko wtedy, gdy $r^{\frac{p-1}{2}} \equiv 1 \pmod{p}$. Jeśli te warunki zachodzą, mówimy, że r jest *resztą kwadratową modulo* p.

Rozwiązanie.

Niech $g \mod p$ będzie generatorem grupy $\mathbb{Z}_p^*$, jak w zadaniu 5. Wtedy mamy równość zbiorów

$$\{1 \mod p, 2 \mod p, \ldots, p-1 \mod p\} = \left\{g \mod p, g^2 \mod p, \ldots, g^{p-1} \mod p\right\},$$

więc $r \equiv g^k \pmod p$ dla pewnej potęgi k. Na mocy wniosku z rozwiązania zadania 5, rząd elementu $r^{(p-1)/2} = g^{k(p-1)/2} \mod p$ to

$$\frac{p-1}{\mathrm{NWD}(p-1, k\frac{p-1}{2})}.$$

Rząd ten wynosi 1 dokładnie wtedy, gdy $\mathrm{NWD}(p-1, k\frac{p-1}{2}) = p-1$, czyli gdy $p-1$ dzieli $k\frac{p-1}{2}$, czyli gdy $k \equiv 0 \pmod 2$. Z drugiej strony, rząd elementu wynosi 1 dokładnie wtedy, gdy ten element to $1 \pmod p$. Udowodniliśmy, że następujące warunki są równoważne

- $r^{\frac{p-1}{2}} \equiv 1 \pmod p$,
- $r \equiv g^k \pmod p$, gdzie k jest parzyste.

Jeśli zatem $r^{\frac{p-1}{2}} \equiv 1 \pmod p$, to można wziąć $a = g^{k/2}$. Jeśli zaś $r \equiv a^2 \pmod p$, to

$$r^{\frac{p-1}{2}} \equiv (a^2)^{\frac{p-1}{2}} = a^{p-1} \equiv 1 \pmod p,$$

z małego twierdzenia Fermata.

Zadanie 8. Niech p będzie pierwsza, a k całkowita dodatnia. Jaka jest reszta z dzielenia przez p liczby $1^k + 2^k + \ldots + (p-1)^k$?

Rozwiązanie.

(To zadanie będzie jeszcze użyte w poniedziałek.)

Zadanie 9 ($p = 4k+1 \iff p = a^2 + b^2$)**.** Niech $\mathbb{Z}[i] \subseteq \mathbb{C}$. Z algebry I wiadomo, że jest to dziedzina z jednoznacznością rozkładu. Niech p będzie liczbą pierwszą taką, że $p \equiv 1 \pmod 4$.

(a) Pokaż, że -1 jest resztą kwadratową modulo p, powiedzmy $c^2 \equiv -1 \pmod p$.

(b) Z równania $(c+i)(c-i) = kp$, dla $k \in \mathbb{Z}$, wywnioskuj, że element $p \in \mathbb{Z}[i]$ nie jest pierwszy.

(c) Niech $p = cd$, gdzie $c, d \in \mathbb{Z}[i]$ są nieodwracalne, powiedzmy $c = a + bi$. Pokaż, że $p = a^2 + b^2$.

Rozwiązanie.

Niech $p = 4k+1$. Mamy

$$(-1)^{\frac{p-1}{2}} = (-1)^{2k} = 1 \pmod p,$$

więc z zadania 7 wynika, że istnieje c takie, że $c^2 \equiv -1 \pmod p$. Zapiszmy $c^2 + 1 = kp$, gdzie k jest całkowite. Wtedy $(c+i)(c-i) = kp$.

Ideał $p\mathbb{Z}[i]$ składa się z elementów postaci $a+bi$, gdzie a, b są całkowite, podzielne przez p. W szczególności, $c+i$, $c-i$ nie należą do tego ideału, ale ich iloczyn już tak. To pokazuje, że element p nie jest pierwszy. Z jednoznaczności rozkładu wynika, że p jest rozkładalny w $\mathbb{Z}[i]$, czyli $p = f_1 \cdot f_2$, gdzie $f_1, f_2 \in \mathbb{Z}[i]$ są nieodwracalne. Biorąc normy, otrzymujemy

$$p^2 = |p|^2 = |f_1|^2 \cdot |f_2|^2,$$

gdzie $|f_1|^2 = a^2 + b^2$ dla $f_1 = a + bi$. Skoro f_1, f_2 są nieodwracalne w $\mathbb{Z}[i]$, to $|f_1|^2, |f_2|^2 > 1$ (sprawdź, że jedyne elementy o normie 1 to $\pm 1, \pm i$ i one są odwracalne). Te nierówności pokazują, że $|f_1|^2 = |f_2|^2 = p$. Zatem $p = a^2 + b^2$.