1. Podzielność

Def: Powiemy, że liczba a dzieli liczbę b gdy $a \cdot k = b$ dla pewnej liczby k. Oznaczamy to jako $a|b$.

Przykład: $1|1$ bo $1 \cdot 1 = 1$

$2|6$ bo $2 \cdot 3 = 6$

$-2|6$ bo $(-2)\cdot(-3) = 6$

~~Każd~~ Dla każdego n $n|0$ bo $0 \cdot n = 0$.

Dla każdego n $1|n$ bo $1 \cdot n = n$.

Def: Liczba $d^{\geq 0}$ jest największym wspólnym dzielnikiem liczb a i b gdy $d|a$, $d|b$ oraz dla każdej liczby d' spełniającej $d'|a$ oraz $d'|b$ mamy $d' \leq d$.

Def: Dla liczb a i b kombinacją liniową liczb a i b nazywamy ~~ti~~ każdą liczbę postaci $k \cdot a + l \cdot b$.

Przykład: Niech $a = 7$, $b = 5$. Wtedy następujące liczby są kombinacjami liniowymi:

$$2 = 1 \cdot 7 + (-1) \cdot 5$$

$$4 = 2 \cdot 7 + (-2) \cdot 5$$

$$1 = 3 \cdot 7 + (-4) \cdot 5$$

$$-14 = [(-14) \cdot 3] \cdot 7 + [(-14) \cdot (-4)] \cdot 5$$

Dla $a = 4$, $b = 8$:

$$4 = 1 \cdot 8 + (-1) \cdot 4$$

$$8 = 1 \cdot 8 + 0 \cdot 4$$

$$4 = 0 \cdot 8 + 1 \cdot 4$$

W obu przypadkach udało nam się znaleźć NWD(a,b) jako kombinację liniową a i b. Okazuje się, że zawsze da się tak zrobić.

TW: Dla liczb a i b NWD(a,b) jest najmniejszą dodatnią kombinacją liniową a i b.

W dowodzie tego twierdzenia korzystamy z tw. o dzieleniu z resztą:
Dla dowolnych liczb a i b, $b \neq 0$ istnieją jedyne liczby k i r takie, że

- $k b + r = a$
- $0 \leq r < b$.

Liczbę r nazywamy resztą z dzielenia a przez b.

Dowód TW: Niech $k_0 \cdot a + l_0 \cdot b$ będzie najmniejszą dodatnią kombinacją liniową a i b. Pokażemy, że $k_0 \cdot a + l_0 \cdot b \mid a$. Z tw. o dzieleniu z resztą istnieje n oraz $0 \leq r < k_0 \cdot a + l_0 \cdot b$ takie, że

$n \cdot (k_0 \cdot a + l_0 \cdot b) + r = a$ wtedy mamy

$$r = a - n \cdot (k_0 \cdot a + l_0 \cdot b) = (1 - n \cdot k_0) \cdot a - n l_0 \cdot b$$

Wobec tego r jest kombinacją liniową, która jest mniejsza niż najmniejsza liniowa kombinacja, więc musimy mieć $r = 0$. To oznacza, że

$n \cdot (k_0 \cdot a + l_0 \cdot b) = a$, więc $k_0 \cdot a + l_0 \cdot b \mid a$.

Podobnie uzasadniemy, że $k_0 \cdot a + l_0 \cdot b \mid b$.

Należy teraz pokazać, że jest to największa taka liczba. Musimy tutaj skorzystać z 2 faktów:

1) ~~Jeżeli $a \mid b_1$ oraz $a \mid b_2$ to dla każdej liczb~~
Jeżeli $d \mid a$ oraz $d \mid b$ to dla dowolnych liczb k, l zachodzi $d \mid k \cdot a + l \cdot b$.

2) ~~$a \mid b \geq 0$~~ Dla liczb $d, a \geq 0$ ~~ma~~ takich, że $d \mid a$ zachodzi ~~d~~ $d \leq a$.

Dowody tych faktów zostawiam jako ćwiczenie.
Ustalmy dowolną liczbę $d \geq 0$ taką, że $d \mid a$ oraz $d \mid b$. Z faktu 1 zachodzi $d \mid k_0 \cdot a + l_0 \cdot b$, zatem z faktu 2. mamy $d \leq k_0 \cdot a + l_0 \cdot b$, co kończy dowód.

2. Przystawanie

Interesuje nas teraz reszta z dzielenia przez pewną liczbę p. Potrzebujemy oznaczenia, że liczby a i b mają tę samą resztę z dzielenia przez p.

Def: Dla liczb a, b oraz liczby p ~~nap~~ powiemy, że a przystaje do b modulo p gdy a i b mają tę samą resztę z dzielenia przez p. Piszemy wtedy

$$a \equiv b \ (\text{mod } p).$$

Fakt: Następujące warunki są równoważne:

- $a \equiv b \pmod p$
- ~~a~~ $p \mid a-b$

Dowód: ćwiczenie.

TW: Niech liczby a, a', b, b' są takie, że

$$a \equiv a' \pmod p, \quad b \equiv b' \pmod p$$

Wtedy
$$a+b \equiv a'+b' \pmod p$$
$$a \cdot b \equiv a' \cdot b' \pmod p$$

D-d: Pokażemy, że $a \cdot b \equiv a' \cdot b' \pmod p$. Sumę zostawiona jako ćwiczenie.
~~Sprowadźmy~~ Niech k_a, k_b będą takimi liczbami, że

$$k_a \cdot p = a - a'$$
$$k_b \cdot p = b - b'.$$

Wtedy $a \cdot b - a'b' = a \cdot b - a'b + a'b - a'b' =$
$= (a-a') \cdot b + (b-b')a = k_a \cdot p \cdot b + k_b \cdot p \cdot a =$
$p \cdot (k_a \cdot b + k_b \cdot a)$, więc $p \mid ab - a' \cdot b'$. Zatem na mocy faktu mamy $a \cdot b \equiv a' \cdot b' \pmod p$.

Fakt: Niech p będzie liczbą pierwszą oraz $p \mid ab$ dla pewnych liczb a i b. Wtedy $p \mid a$ lub $p \mid b$.
Dowód pomijamy, bo wymaga rozkładu ~~na~~ liczb na czynniki pierwsze.

Wniosek: Niech p będzie liczbą pierwszą oraz niech $0 < a < p$. Wtedy istnieje liczba c taka, że

$a \cdot c \equiv 1 \pmod p$ gdy $0 < c < p$

Liczbę tą nazywamy odwrotnością a i oznaczamy a^{-1}.

D-d wniosku: Dla a i p jak wyżej mamy $NWD(a,p) = 1$. Wobec tego istnieje liczba c taka, że

$$c \cdot a + l \cdot p = 1$$

To oznacza, że $c \cdot a - 1 = l \cdot p$, więc z faktu wynika, że $c \cdot a \equiv 1 \pmod p$.

Fakt: ~~Istnieją jedynie 2 liczby~~ jeżeli $0 < a < p$ oraz $a^2 \equiv 1 \pmod p$ to $a = 1$ lub $a = p-1$.

Dowód faktu:

Zauważmy, że z $a \cdot b \equiv 0 \pmod p$ wynika, że $a \equiv 0 \pmod p$ lub $b \equiv 0 \pmod p$ (ćwiczenie).

Wobec tego równanie $x^2 - 1 \equiv 0 \pmod p$

$$x^2 - 1 = (x+1)(x-1)$$

Ma 2 rozwiązania: $x = 1$, $x = p-1$.

TW (Wilson) Dla liczby pierwszej p mamy

$$(p-1)! \left(= 1 \cdot 2 \cdot 3 \cdot \ldots \cdot (p-1)\right) \equiv -1 \pmod p$$

D-d: $p=2$: $(p-1)!=1$, $1-(-1)=2 \mid 2$ ok!

~~prz~~: $p=3$: $(p-1)!=2$, $2-(-1)=3 \mid 3$ ok!

$p>3$: Dla tych liczb p są liczby ~~p~~ $1<a<p-1$.
Z przedstawionych wyżej faktów wynika, że

$$2\cdot 3\cdot\ldots\cdot(p-2)\equiv 1 \pmod p\text{, ponieważ}$$

każda z tych liczb ma wśród nich swoją odwrotność multiplikatywną modulo p. Zatem

$$1\cdot 2\cdot 3\cdot\ldots\cdot(p-2)\cdot(p-1)\equiv -1 \pmod p.$$

Fakt: Niech $r_p(n)$ oznacza resztę z dzielenia n przez p (patrz tw. o dzieleniu z resztą). Wtedy dla dowolnej liczby $0<a<p$ zachodzi

$$\{\cancel{0}, 1, \ldots, p-1\}=\{r_p(a\cdot 1), r_p(a\cdot 2), \ldots, r_p(a\cdot(p-1))\}$$

D-d: Samo ćwiczenie.

Wniosek (Małe tw. Fermata): ~~Niech $0<a<p$~~
Niech ~~$0\leq a\leq$~~ $0\leq a<p$ ~~będzie dowolną~~ liczbą. Wtedy

$$a^p\equiv a \pmod p.$$

D-d: $p \mid a$ wtedy $p \mid a^p$. ok

Jeżeli p nie dzieli a to z faktu mamy

$$1\cdot 2\cdot\ldots\cdot(p-1)\equiv r_p(a\cdot 1)\cdot r_p(a\cdot 2)\cdot\ldots\cdot r_p(a(p-1))\equiv$$
$$\equiv a\cdot(2\cdot a)\cdot(3\cdot a)\cdot\ldots\cdot(p-1)a=a^{p-1}\, 1\cdot 2\cdot 3\cdot\ldots\cdot(p-1).\text{ Zatem}$$
$$1\equiv a^{p-1}\text{, więc } a\equiv a^p \pmod p.$$