① Делимост при целите числа. Най-голям общ делител, тождество на Безу. Простите числа и основна теорема на аритметиката.

Th (Деление с частно и остатък)
Нека $a, b \in \mathbb{Z}$, $b \neq 0$.
Тогава, $\exists! q, r \in \mathbb{Z} : a = bq + r$, $0 \leq r < |b|$, където q - частно, r - остатък.

Доказателство:
$\exists$) Нека $M = \{ a - bs \mid s \in \mathbb{Z} \}$
Тъй като в M има както положителни, така и отрицателни числа, а ние се интересуваме само от неотрицателните, отделяме от M множеството M^+: $M^+ = \{ x \in M \mid x \geq 0 \}$.
Нека r е най-малкото в M^+, тогава $r - |b| < 0$
$\Rightarrow r < |b| \Rightarrow 0 \leq r < |b|$ и $a - b.s_1 = r \Rightarrow a = b.s_1 + r$

!) $a = b.q_1 + r_1$, $0 \leq r_i < |b|$
$a = b.q_2 + r_2$
$0 = b(q_1 - q_2) + r_1 - r_2$
$\Rightarrow b(q_1 - q_2) = r_2 - r_1$
Ако $q_1 - q_2 \neq 0$, то $|b(q_1 - q_2)| \geq |b|$, но $r_2 - r_1 < |b|$
$\Rightarrow q_1 - q_2 = 0 \Rightarrow q_1 = q_2$, $r_1 = r_2$

Следствие: (Представяне на числата в q-ична бройна система)
Нека $b > 1$, $b \in \mathbb{N}$, $a \in \mathbb{N}$
Тогава $\exists! q_0, q_1, \ldots, q_\ell : a = q_0 + q_1 b + q_2 b^2 + \ldots + q_\ell b^\ell$, където $0 \leq q_i < b$, $q_\ell \neq b^\ell$.

Доказателство: (по индукция)
I стъпка: $a = q_0 + ba_1$, $0 \leq q_0 < b$
II стъпка: $a_1 = q_1 + ba_2$, $0 \leq q_1 < b$
$\vdots$ докато $a_i \geq b$

Опр.|| Казваме, че числото b дели числото a ($b|a$) или числото a се дели на числото b ($a:b$), когато $a = bq$, $b \neq 0$.

Свойства: (на делимостта)

1) $\pm 1 | a, \forall a \in \mathbb{Z}$;
2) $a | \pm a, \forall a \neq 0$;
3) $a | 0, \forall a \neq 0$;
4) $a|b, b|c \Rightarrow a|c$;
5) $a|b \Rightarrow a|bu$;
6) $a|b_1, a|b_2 \Rightarrow a|b_1u_1 + b_2u_2$;
7) $a|b, b \neq 0 \Rightarrow |a| \leq |b|$.

Опр.|| $НОД(a,b) = (a,b) = d$, където d е max : $d|a$, $d|b$ или алтернативното определение, което ще бъде обобщено за полиноми:

$НОД(a,b) = (a,b) = d$:

1) $d|a$, $d|b$;
2) ако $d_1|a$, $d_1|b \Rightarrow d_1|d$.

При второто определение се получава както общият общ делител d, така и $-d$. Двете определения са еквивалентни с точност до знак.

Th|| (Безу)

Ако $a, b \in \mathbb{Z}$, поне едното е различно от 0, то $\exists (a,b) = d$ и $\exists u, v \in \mathbb{Z}$: $d = ua + vb$, където $d = ua + vb$ се нарича „тъждество на Безу".

Доказателство:

Нека $M = \{ as + bt \mid s, t \in \mathbb{Z} \}$

Тъй като в M има както положителни, така и отрицателни числа, а ние се интересуваме само от

положителните, отделяне от M множеството M^+: $M^+ = \{x \in M \mid x > 0\}$.
Нека d е min число в $M^+ \Rightarrow d > 0$.
Тъй като d е от $M^+ \subset M$, то d може да се представи като $d = au + bv$. Тъй като няма единственост на u, v, остава да докажем, че $d = НОД(a,b)$.
$\forall x \in M \; \exists! \, q, r : x = dq + r, \; 0 \le r < d$
$\Rightarrow x = as_1 + bt_1 = (au + bv)q + r$
$\Rightarrow r = (s_1 - uq)a + (t_1 - vq)b \in M$, но $0 \le r < d$, а d е min положително число от $M \Rightarrow r = 0$
$\Rightarrow x = dq \Rightarrow d \mid x, \; \forall x \in M \Rightarrow d \mid a, d \mid b$.
Ако $d_1 \mid a, d_1 \mid b \Rightarrow d_1 \mid au + bv \Rightarrow d_1 \mid d, d > 0$:
1) $d \mid a, d \mid b$;
2) ако $d_1 \mid a, d_1 \mid b \Rightarrow d_1 \mid d \Rightarrow d = НОД(a,b)$.

Опр.|| Числата a и b са взаимно прости, когато $(a,b) = 1$.

Следствие 1: $a \mid b_1 b_2, \; (a, b_1) = 1 \Rightarrow a \mid b_2$
Доказателство:
$a \mid b_1 b_2, \; (a, b_1) = 1 \Rightarrow 1 = au + b_1 v \Rightarrow b_2 = ab_2 u + b_1 b_2 v$
$\Rightarrow a \mid b_2$

Следствие 2: $a_1 \mid b, \; a_2 \mid b, \; (a_1, a_2) = 1 \Rightarrow a_1 a_2 \mid b$
Доказателство:
$a_1 \mid b \Rightarrow b = a_1 . s$, но $a_2 \mid b \Rightarrow a_2 \mid a_1 . s \Rightarrow a_2 \mid s \Rightarrow$
$\Rightarrow s = a_2 t \Rightarrow b = a_1 a_2 t \Rightarrow a_1 a_2 \mid b$

Опр.|| Числото $p \in \mathbb{Z}$ е просто, ако p се дели само на ± 1 и $\pm p$.

(Тв.) Простите числа са безкраен брой.

Доказателство:

Допускаме, че са краен брой $p_1, \dots, p_n$. Тогава $A = p_1 \dots p_n + 1$ не се дели на нито едно просто число.

Th. II (Основна теорема на Аритметиката)

Всяко естествено число по-голямо от единица може да се представи като произведение на прости числа (множители), като това представяне е единствено с точност до реда на множителите.

Доказателство:

∃) (индукция по a)

База: $a = 2 \Rightarrow a$ е просто

ИП: Чека е в сила за всички числа по-малки от a:

1 случай: a е просто, то тогава $= p$

2 случай: a не е просто (т.е. a е съставно), то тогава

$$\exists b, c : a = b.c,\ b < a,\ c < a$$

ИС: Прилагаме ИП за b, c, т.е. $b = p_1 \dots p_r$, $c = q_1 \dots q_s$, p_i, q_j - прости

Тогава $a = b.c = p_1 \dots p_r . q_1 \dots q_s$ - прости множители

!) Да допуснем, че $a = p_1 \dots p_e$ и $a = q_1 \dots q_t$, p_i, q_j - прости множители $\Rightarrow p_1 \dots p_e = q_1 \dots q_t \Rightarrow q_t \mid q_1 \dots q_t \Rightarrow$

$\Rightarrow q_t \mid p_1 \dots p_e$

Тъй като q_t е просто число, то q_t трябва да дели някое p_i, но всяко p_i е просто $\Rightarrow \exists$ номер $i : p_i = q_t$. С преномериране на $p_1 \dots p_e$, може да считаме, че $p_e = q_t$.

Това ~~~~ означава, че $(p_1 \dots p_{e-1}) p_e = (q_1 \dots q_{t-1}) q_t \Rightarrow$

$\Rightarrow p_1 \dots p_{e-1} = q_1 \dots q_{t-1}$.

Ако $l > t$, то $p_1 \dots p_{e-t} = 1$ ⚡ $\Rightarrow l = t$.

Тогава след преномерирането на едната страна, накрая ще получим, че $p_i = q_i$, $i = 1, \dots, t$.