1) prvočísla
2) kongruence

$p \in \mathbb{N}$: $1|p$ $p|p$ a nic jiného

Euklid: $p_1|\dots|p_N$ všechna

$K = p_1 p_2 \cdots p_N + 1$ $\Rightarrow$ spor

q q

$a \in \mathbb{N}$ $a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_k^{\alpha_k}$

$a+1 = p \cdot q$ $p < a$, $q < a$

2 27-15:59

10.8. $n > 2$ $n!$ mezi nimi bude prv.

3 6
4 24

Uvažme $n!-1$, $p \mid n!-1$

1) $p \le n \Rightarrow p \mid n! \Rightarrow$ nedělí $n!-1$ spor

2) $p > n$ $p \le n!-1$

10.9. $\forall n \exists$ n po sobě jdoucích "neprvočísel"

$(n+1)!+2,\ (n+1)!+3,\ \dots,\ (n+1)!+n+1$

$k \in \{2, \dots, n+1\}$ $k \mid (n+1)!$ $k \mid (n+1)!+k$

2 27-16:11

počet prvoč. $\le x$ je přibližně

$\pi(x) \approx \frac{x}{\ln x}$

x	$\pi(x)$	$x/\ln x$
100	25	21,71
10000	1229	1085,73
500000	41538	38102,89

$m = 3$
$(2,3) = 1$
$1 = k \cdot 2 + l \cdot 3$
$k = 2$ $l = -1$
mod 3:
$1 = (2) \cdot 2$

Bezout: $(a,b) = k \cdot a + l \cdot b$ $1 = ka$ mod b $1 = kb$

2 27-16:22

$5k + 3k = 4$

$5k = 4 \mod 3$

$2k = 1 \mod 3$

$2^{-1} = 2 \mod 3$

$\Rightarrow k = 2 + r3$

modul m $x \equiv y \mod m$

$\Leftrightarrow x - y = r \cdot m$

$m=3$

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

·	0	1	2
0	0	0	0
1	0	(1)	2
2	0	2	(1)

$m=2$

+	0	1
0	0	1
1	1	0

·	0	1
0	0	0
1	0	1

2 27-16:25

10.11. (i) $7^{30} \mod 50$?

$7^2 = 49 = -1 \mod 50$

$7^{30} = (7^2)^{15} = (-1)^{15} = -1 \mod 50$

$6 = 2 \mod 4$

$3 \equiv 1 \mod 2$

(ii) 7^{30} .. jaké jsou 2 poslední cifry

tj. $7^{30} \mod 100$? $100 = 2 \cdot 50 = 2 \cdot 2 \cdot 5^2$

$7^{30} = 49 \mod 50 \Rightarrow 7^{30} = (49) = -1 \mod 100$

$\Rightarrow 7^{30} = (7^2)^{15} = (-1)^{15} = (-1) \mod 25$

$7^{30} = (-1)^{30} = (1) \mod 4$

a jedno z nich

$\Rightarrow 7^{30} = 49 \mod 100$

2 27-16:39

7^{30} 2-cifr, končící 2

mod 4: $7^{30} = (-1)^{30} = 1$ 01

mod 8: $7^{30} = (-1)^{30} = 1$ 001

mod 16: $7^2 = (+1)$

$7^{30} = (+1)^{15} = +1$ 0001

~~mod 52~~: nějaké 9, 2 cifry

$7 = -2$ $7^{30} = (-2)^{30} = 2^{30} = (2^5)^{10} = (-1)^{10} = 1$

2 27-16:51

10.12. $37^{m+2}+16^{m+1}+23^m \mod 7$?

$37 = 35+2 \quad 16 = 14+2 \quad 23 = 21+2$

$2^{m+2}+2^{m+1}+2^m = 2^m(4+2+1) = 7\cdot 2^m$

$= 0 \mod 7$

10.13 $m = (835^5+6)^{18}-1$ je dělitelné 112 ?

$112 = 7\cdot 16 \quad 7 \mid m \;?\; 16 \mid m \;?$

7: $m \equiv (2^5+6)^{18}-1 = (38)^{18}-1 = 3^{18}-1 = (-1)^6-1 = 0$

16: $m \equiv (3^5+6)^{18}-1 = (3\cdot 81+6)^{18}-1$

$= 9^{18}-1 = 1^9-1 = 0$

2 27-16:58

$x \equiv y \mod a \quad (a,b)=1 \Rightarrow x \equiv y \mod a\cdot b$

$x \equiv y \mod b$

$x-y = r\cdot a = s\cdot b \Rightarrow r = b\cdot t$

$\Rightarrow x-y = t\,[a\cdot b]$

pravidla dělitelnosti:

~~3~~, 9: $m = a_k 10^k + a_{k-1}10^{k-1} + \dots + a_0 10^0$

$10 \equiv 1 \mod 3$ $S(m) = a_k + a_{k-1} + \dots + a_0 \equiv n \mod 9$

$10 \equiv 1 \mod 9$ $\mod 3$

$10 \equiv -1 \mod 11$ $T(m) = a_0 + a_2 + \dots - a_1 - a_3 - \dots \equiv n \mod 11$

$-2-1+3 = 0$ [2013]

2 27-17:11

$100 \equiv 2 \mod 7$

$1001 = 7\cdot 11\cdot 13$

$m = 1000a + b$

$m \equiv -a+b \mod 7, 11, 13$

$17\cdot 6 = 102 \quad m = a\,100 + b$

$m = -2a+b \mod 17$

$m = 20\cdot 100 + 17 \equiv -40+17 \equiv 11 \mod 17$

2 27-17:22

$2^q - 1$ Mersennovo prvočíslo

6 $1, 2, 3, 6$ součet dělitelů je $12 = 2\cdot 6$

dokonalé číslo

Věta Sudé číslo n je dokonalé $\Leftrightarrow n = 2^{q-1}(2^q-1)$, 2^q-1 prvočíslo

2 27-17:30