# Number Theory

1 gcd: $d$ is the gcd of $a, b \in \mathbb{Z}$

1 $d \mid a$

2 $d \mid b$

3 $q \in \mathbb{Z}$ $q \mid a \wedge q \mid b \Rightarrow q \mid d$

↳ find w/ Euclidean Alg (Big Thm) general ★
can also be used (exam2)

↳ find specific soln to $ax + by = c$ w/ reverse Euclidean alg

★ Bezout's Lemma: sol to $ax + by = c \Leftrightarrow \gcd(a,b) \mid c$

↳ display thm to get all solns

$$x = x_0 + k \frac{b}{\gcd(a,b)} \qquad y = y_0 - k \frac{a}{\gcd(a,b)} \qquad k \in \mathbb{Z}$$

2 prime #'s $p$ ★

1 $p \mid ab \Rightarrow p \mid a \vee p \mid b$ (def of prime)

2 $p = mn \Rightarrow m$ or $n$ unit (def of irreducible)

↳ coprime: $a \perp b \Leftrightarrow \gcd(a,b) = 1$

★ ↳ unique prime factorization: $n \in \mathbb{Z}$ $n > 1$
n can uniquely be represented as the prod of primes

coprime:

★ ↳ coprime lemma: ~~[illegible]~~ $a \perp b$ $a \mid bc \Rightarrow a \mid c$

3 modular arithmetic: $a, b, n \in \mathbb{Z}$ $a \equiv b \bmod n$

$\Leftrightarrow$ $n \mid a - b \Leftrightarrow a - b = nk, k \in \mathbb{Z} \Leftrightarrow a = b + nk$ $k \in \mathbb{Z}$

↳ CAN ONLY

$a + c \equiv b + c$

$ac \equiv bc$

$a - c \equiv b - c$

NO

$c^a \equiv c^b$

~~[illegible]~~

$a/c \equiv b/c$

mod cont.

↳ FLT : for prime $p$, $a \in \mathbb{Z}$ $\quad a^p \equiv a \mod p$

~~or~~ AND ALSO

when $a \perp p$ $\quad a^{p-1} \equiv 1 \mod p$

↳ wanna mult by $a^{-1}$ on both sides so $a \perp p$ req.

↳ Euler's Thm (general FLT)

↳ Wilson's Thm : for prime $p > 1$ $\quad (p-1)! \equiv -1 \mod p$

↳ pf of Wilson's : each # gets matched to their inverses except $(p-1)$ so it is $-1$ $(2 - p-2)$

problems :

① Prove $n^7 - n$ is divisible by 42 $\forall n \in \mathbb{N}^+$

$\Rightarrow 42 \mid n^7 - n$

$\Rightarrow n^7 \equiv n \mod 42$ $\quad \varphi(42) = \cancel{20}\ 12$ ̈n

$42 = 7 \cdot 3 \cdot 2$ so

$42 \mid n^7 - n \iff 7 \mid n^7 - n \wedge 3 \mid n^7 - n \wedge 2 \mid n^7 - n$

$n^7 - n \equiv n - n \mod 7$ (FLT) general case cuz $a \not\perp p$

$\equiv 0 \mod 7$ ✓

$n^7 - n \equiv (n^3)^2 \cdot n - n \mod 3$ (FLT) $\equiv n^2 \cdot n - 2 \mod 3$ (FLT)

$\equiv n - n \equiv 0 \mod 3$ ✓

$2 \mid n^7 - n$ b/c $n^7$ & $n$ have same parity

so diff will be even ✓

② Let $a$ be an int ST $\frac{1}{1}+\frac{1}{2}+\ldots+\frac{1}{23}=\frac{a}{23!}$

Find the remainder of $a$ when divided by 13

$$\frac{1}{1}+\frac{1}{2}+\ldots+\frac{1}{23}=\frac{a}{23!}$$

$$\Rightarrow \frac{23!}{1}+\frac{23!}{2}+\ldots+\frac{23!}{23}=a$$

$$\Rightarrow a \equiv \frac{23!}{13} \mod 13$$

$$\Rightarrow a \equiv 12! \cdot 14 \cdot 15 \cdot \ldots \cdot 23 \mod 13$$

$$\equiv 12!\,(1 \cdot 2 \cdot \ldots \cdot 10) \mod 13$$

$$\equiv -1 \cdot 10! \mod 13 \quad \text{(Wilson's)}$$

$$\equiv -1 \cdot 10! \cdot 11 \cdot 11^{-1} \cdot 12 \cdot 12^{-1} \mod 13 \qquad 12 \equiv -1 \mod 13$$

$$\equiv -1 \cdot 12! \cdot 11^{-1} \cdot 12^{-1} \mod 13 \qquad \Rightarrow 12^{-1} \equiv -1 \mod 13$$

$$\equiv -1 \cdot 12!\,(-1)(-7) \mod 13 \quad \text{(Wilson's)}$$

$$\equiv (-1)(-1)(-1)(-7) \mod 13 \qquad 11 \equiv -2 \mod 13$$

$$\equiv 7 \mod 13 \ \checkmark \qquad \Rightarrow 11^{-1} \equiv -7 \mod 13$$