Jan 23rd

Ex: $3^{2n+1}+2^{2n+1}$ is divisible by 5 for any n.
$3^{2n}\cdot 3+2^{2n}\cdot 2=(3^2)^n\cdot 3+(2^2)^n\cdot 2$

$3^2\equiv -1 \pmod 5$
$2^2\equiv 4\equiv -1 \pmod 5$
$(3^2)^n\equiv(-1)^n \pmod 5$
$(2^2)^n\equiv(-1)^n \pmod 5$
$3^{2n+1}+2^{2n+1}\equiv 3(3^2)^n+2(2^2)^n \pmod 5 \equiv (-1)^n\cdot(3+2) \pmod 5$
$\equiv 0 \pmod 5$

Little Fermat's Theorem

Let p be a prime # and a - natural number not divisible by p
Then $a^{p-1}\equiv 1 \bmod p$

Ex: $p=5, a=3$ $3^4\equiv 1 \bmod 5$
$p=5, a=2$ $2^4\equiv 1 \bmod 5$

Proof: $a1 \bmod p, a2 \bmod p, \dots, a(p-1) \bmod p$
↳ p-1 mods

Claim: These are all distinct mod p.

$1\le k<l\le p-1$
if $a\cdot k\equiv a\cdot l \pmod p$
$ak-al$ is divisible by p
$p\mid a(k-l) \Rightarrow p\mid k-l$
↑ prime $p\nmid a$
$0<l-k\le p-1$ is not divisible by p.

$p=7, a=2$
$2\cdot 1 \bmod 7=2 \bmod 7$
$2\cdot 2 \equiv 4 \bmod 7$
$2\cdot 3\equiv 6 \bmod 7$
$2\cdot 4\equiv 1 \bmod 7$
$2\cdot 5\equiv 3 \bmod 7$
$2\cdot 6\equiv 5 \bmod 7$
all distinct mod 7

there are p equivalance classes mod p.
$0 \bmod p, 1 \bmod p, \dots (p-1) \bmod p$
there are only $(p-1)$ non-zero equivalance classes mod p
$1 \bmod p, \dots, (p-1) \bmod p$

$\Rightarrow a1 \bmod p, \dots, a(p-1) \bmod p$

"one-to-one" for $(p-1)$ pairs

the same as $1 \bmod p, \dots (p-1) \bmod p$

Ex:
for $p=7$, $a=2$

$2\cdot1 \bmod 7$ $2\cdot2 \bmod 7$ $2\cdot3 \bmod 7$ $2\cdot4 \bmod 7$ $2\cdot5 \bmod 7$ $2\cdot6 \bmod 7$

$1 \bmod 7$ $2 \bmod 7$ $3 \bmod 7$ $4 \bmod 7$ $5 \bmod 7$ $6 \bmod 7$

Why they go to different "baskets"?
i.e. no "2" go to "1"
$a\cdot1 \bmod p, \dots, a(p-1) \bmod p$ are all distinct modular
same as $1 \bmod p$, $2 \bmod p \dots (p-1) \bmod p$ in some orders.

$1 \le k < l < p-1$
if $a\cdot k \equiv a\cdot l \bmod p$
$p \mid al - ak = a(l-k)$
$p \nmid a \Rightarrow p \mid l-k$
$\Rightarrow (a\cdot1)(a\cdot2)\cdots(a\cdot(p-1)) \equiv 1\cdot2\cdots(p-1) \pmod p$
$a^{p-1}(1\cdot2\cdots(p-1)) \equiv 1\cdot2\cdots(p-1) \bmod p$
$p \mid a^{p-1}(p-1)! - (p-1)! = (p-1)!(a^{p-1}-1)$
$\Rightarrow p \mid (p-1)!$ or $p \mid a^{p-1}-1 \Rightarrow p \mid a^{p-1}-1$

$\Rightarrow a^{p-1} \equiv 1 \bmod p$

Corollary: Let p be prime
then $a^p \equiv a \pmod p$ for any a
$2^4 \equiv 2 \bmod 7$, $3^5 \equiv 3 \bmod 5$

Pf: Two cases
① a is divisible by $p \Rightarrow a^p \equiv a \equiv 0 \bmod p$
② a is not divisible by $p \Rightarrow a^{p-1} \equiv 1 \bmod p \times a$
forms $a^p \equiv a \bmod p$

Corollary: For any a not divisible by p (prime), there exists $1 \le b \le p-1$
s.t. $a\cdot b \equiv 1 \bmod p$

Proof: $a^{p-1} = a\cdot a^{p-2} \equiv 1 \bmod p$ by Fermat
take $b = a^{p-2} \bmod p$

Ex: $a=2$, $p=5$
$a^{p-2} \equiv 2^3 \bmod 5 \equiv \underbrace{3 \bmod 5}_{\hookrightarrow b}$

$2\cdot3 \equiv 6 \equiv 1 \bmod 5$ ✓

Ex: $a=3$, $p=7$. $a^{p-2} \equiv 3^5 = 243 \bmod 7 \equiv \underbrace{5 \bmod 7}_{\hookrightarrow b}$

$3\cdot5 \equiv 15 \bmod 7 \equiv 1 \bmod 7$ ✓

Let p be prime

a not divisible by $p \Rightarrow$

can solve $ax \equiv b \bmod p$ for any b

and the solution is unique mod p.

First solve $ax \equiv 1 \bmod p$ $\quad x \equiv a^{p-2} \bmod p$ mod p works

$a \times b \equiv b \bmod p$

Ex: $2x \equiv 3 \bmod 7$

$x = 5$ works $2 \cdot 5 \equiv 10 \equiv 3 \bmod 7$

If $ax_1 \equiv ax_2 \equiv b \bmod p$

two solutions $\Rightarrow$

$p \mid ax_1 - ax_2 = a(x_1 - x_2) \Rightarrow p \mid x_1 - x_2 \Rightarrow x_1 \equiv x_2 \bmod p$

$p \nmid a$

$x \equiv b \bmod p$ not always solvable

and can have several solutions

we checked before that

$x^2 \equiv 3 \bmod 4$ has no solutions

Lemma: $x^2 \equiv 1 \bmod p$

iff $x \equiv \pm 1 \bmod p$

if $x = \pm 1 \bmod p \Rightarrow x^2 = (\pm 1)^2 \equiv +1 \bmod p$

if $x^2 \equiv 1 \bmod p \Rightarrow p \mid x^2 - 1 = (x-1)(x+1) \Rightarrow p \mid (x-1)$ or $p \mid (x+1)$

$\Rightarrow x \equiv 1 \bmod p$ or $x \equiv -1 \bmod p$

(prime)

Note:

$ax \equiv 1 \pmod p$ if p is not prime

might not have any solutions!

ex: $2x \equiv 1 \bmod 6$

$2x - 1$ is odd $\Rightarrow$ can not be divisible by 6

ex:

$n^7 - n$ is divisible by 21. (by 3 & by 7)

$n^7 - n$ is divisible by 7 by Fermat

$p = 7$ is prime $\Rightarrow$

$n^7 \equiv n \bmod 7 \Rightarrow$

$n^7 - n$ is divisible by 7

divisible by 3?

Case 1: yes. $\Rightarrow$ divisible by 3

Case 2: No. $\Rightarrow n^{3-1} \equiv 1 \bmod 3$

$n^2 \equiv 1 \bmod 3$

$(n^2)^3 \equiv 1^3 \equiv 1 \bmod 3$

$n^6 \equiv 1 \bmod 3$

$\Rightarrow n \cdot n^6 \equiv n \cdot 1 \bmod 3$

$n^7 \equiv n \bmod 3$

$3 \mid n^7 - n$

$7 \mid n^7 - n$ $\Rightarrow 21 \mid n^7 - n$

Wilson's Theorem

Let p be prime then $(p-1)! \equiv -1 \pmod p$

Ex: $p=3$ $(3-1)! = 2! = 2 \equiv -1 \bmod 3$

Proof: $1 \bmod p, 2 \bmod p, \cdots, (p-1) \bmod p$

$1 \le a \le p-1$

$\Rightarrow \exists\ 1 \le b \le p$ s.t. $ab \equiv 1 \bmod p$

For any $1 \le a \le p-1$ we pair it up with $1 \le b \le p-1$ s.t. $a \cdot b \equiv 1 \bmod p$

Take $p=7$ as an example again:

$1 \bmod 7, 2 \bmod 7, 3 \bmod 7, 4 \bmod 7, 5 \bmod 7, 6 \bmod 7$

Which numbers pair up with themselves?

$a \cdot a \equiv 1 \bmod p$

i.e. a solves $x^2 \equiv 1 \bmod p$

can only happen if $a \equiv \pm 1 \bmod p$

$(p-1)! = 1 \cdot 2 \cdot 3 \cdot 4 \cdots (p-1) \equiv 1 \cdot (p-1) \equiv p-1 \equiv -1 \bmod p$

all the # other than 1 & $p-1$ come in pairs

$a \ne b$ s.t. $a \cdot b \equiv 1 \bmod p$

same proof $\Rightarrow$ if $p > 2$ prime $\Rightarrow (p-2)! \equiv 1 \bmod p$

What if p is not prime?

Theorem: $m>4$ composite $\Rightarrow (m-1)! \equiv 0 \bmod m$

Proof: m is composite $\Rightarrow m = a \cdot b$, $1<a,b<m$

if $a \neq b$, $(m-1)! = 1 \cdot 2 \cdots a \cdots b \cdots (m-1)$

$\Rightarrow$ divisible by a, b

if $a=b$, $m=a^2$

$m>4$, $a=\sqrt{m}>2$

$(m-1)! = 1 \cdot 2 \cdot 2 \cdots (a) \cdots (2a) \cdots (m-1)$

$2a < a^2 = m$

so divisible by $a^2 = m$

Ex: $m=6$

$(6-1)! = 5! = 120 = 6 \cdot 20$ divisible by 6

$m=4$

$(4-1)! = 6 = 2 \times 3 = 2 \bmod 4$

$$\Rightarrow (m-1)! = \begin{cases} -1 \bmod m \text{ if } m \text{ is prime} \\ 2 \bmod m \text{ if } m=4 \\ 0 \bmod m \text{ if } m>4 \text{ composite} \end{cases}$$

Ex: $(10! \cdot 16 + 43)^{202} \bmod 11 = ?$

$43 \equiv -1 \bmod 11$

11 is prime

$10! \equiv -1 \bmod 11$

$16 \equiv 5 \bmod 11$

$10! \cdot 16 + 43 \equiv (-1) \cdot 5 + (-1) \bmod 11 \equiv -5 - 1 \equiv -6 \equiv +5 \bmod 11$

$(10! \cdot 16 + 43)^{202} \equiv 5^{202} \bmod 11$

$5^{11-1} \equiv 1 \bmod 11$ $\quad 5^{10} \equiv 1 \bmod 11$ by Fermat

$5^{10k} \equiv (5^{10})^k \equiv 1^k \equiv 1 \bmod 11$

$5^{202} \equiv (5^{10})^{20} \cdot 5^2 \equiv 1^{20} \cdot 5^2 \equiv 25 \bmod 11 \equiv 3 \bmod 11$

Greatest common divisors

a, b — natural #

$(a,b) = \gcd(a,b)$ def'n: largest natural # that divides both a & b

Ex: $\gcd(4,6) = 2$

$\gcd(12,18) = 6$

Theorem: Let $a = p_1^{k_1} \cdots p_t^{k_t}$

$b = p_1^{m_1} \cdots p_t^{m_t}$

$p_1, \ldots, p_t$ primes

Then $\gcd(a,b) = p_1^{\min(k_1,m_1)} p_2^{\min(k_2,m_2)} \cdots p_t^{\min(k_t,m_t)}$

ex: $\gcd(4,6)$

$4 = 2^2 \cdot 3^0$

$6 = 2^1 \cdot 3^1$

$\gcd(4,6) = 2^1 \cdot 3^0 = 2 \cdot 1 = 2$ ✓