Jan 28th

About Fermat's Little Theorem :

If $\gcd(a,p)=1$ then $a^{p-1}\equiv 1 \bmod p$ — prime case

If $\gcd(a,n)=1$ then $a^{\varphi(n)}=1 \bmod n$ — general case

$\varphi(n)=\#\{k<n : \gcd(k,n)=1\}$

$10^{10} \bmod 11$

Note: $\gcd(10,11)=1$, 11 is prime

$10^{10}\equiv 1 \bmod 11$

$10^{10^{10}} \bmod 11$ $\qquad 10^{10^9\cdot 10}\equiv (10^{10})^{10^9}\equiv 1^{10^9}\equiv 1 \bmod 11$!!!

$10^{5^5} \bmod 11$

compute $5^5 = 10k+n$

compute $5^5 \bmod 10$

$5^2\equiv 25\equiv 5 \bmod 10$

$5^5\equiv (5^2)^2 5 \equiv 5^2\cdot 5\equiv 5\cdot 5\equiv 5 \bmod 10$

$5^5\equiv 5 \bmod 10$

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

Problem Set III

#1.

$a^{p^{p-1}} \bmod p$? $\equiv a^{k(p-1)+1}\equiv a^1 \bmod p\equiv a$

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

$\equiv (p-1+1)^{p-1} \bmod p-1$

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

$\equiv 1$

$p^{p-1}\equiv k(p-1)+r$

Want. $p^{p-1} \bmod p \equiv (p-1+1)^{p-1}\equiv 1^{p-1}$

$a^{p^{p-1}}\equiv a^{k(p-1)+1}\equiv (a^{p-1})^k\cdot a^1$

$\equiv 1^k\cdot a^1 \bmod p$ — Fermat

$\equiv a \bmod p$

Wilson's Theorem

p is prime $\Longleftrightarrow (p-1)!\equiv -1 \bmod p$

$(5-1)!\equiv 4!$

$\equiv 1\cdot 2\cdot 3\cdot 4 \bmod 5$

$\equiv 1\cdot 1\cdot 4$

$\equiv 4$

so 5 is prime !

compute $(12!)^{6!} \bmod 13\equiv (12)^{6!}\equiv (13-1)^{6!}\equiv (-1)^{6!}\equiv 1 \bmod 13$

Another problem from PS:

$1+2+2^2+\cdots+2^{219} \bmod 13$

every 12 is a cycle

$219 = k \cdot 12 + r$

not an appropriate method

n	$2^n \bmod 13$
1	2
2	4
$\vdots$	$\vdots$

$$1+x+x^2+\cdots+x^n = X$$

$$(1-x)(1+x+x^2+\cdots+x^n) = (1-x)X$$

$$1+x+x^2+\cdots+x^n - x - x^2 - \cdots - x^n - x^{n+1} = (1-x)X$$

$$X = \frac{1-x^{n+1}}{1-x}$$

so $1+2+2^2+\cdots+2^{219} = \dfrac{1-2^{220}}{1-2} = 2^{220}-1$

$$2^{220}-1 \bmod 13 \equiv (2^4)-1 \bmod 13 \equiv 2 \bmod 13$$

If $2^{ab}+1$ and b odd consider $2^{ab}+1 \bmod 2^a+1 \equiv (2^a)^b+1 \equiv (2^a+1-1)^b+1$

$\equiv (-1)^b+1$

$\equiv -1+1$

$\equiv 0$

$2^a+1 \mid 2^{ab}+1$ if b is odd

$1 \leq 2^a+1 < 2^{ab}+1$