Some Examples (Section 5.3)

① Illustration of the proof for Wilson's theorem

→ Read Example 5.1 for $p=13$

→ For $p=17$

In $2, 3, \cdots, \underbrace{15}_{p-2}$ there are $\frac{p-3}{2} = 7$ pairs of mutual multiplicative inverses as follows

$2 \cdot 9 \equiv 1 \pmod{17}$
$3 \cdot 6 \equiv 1 \pmod{17}$
$4 \cdot 13 \equiv 1 \pmod{17}$
$5 \cdot 7 \equiv 1 \pmod{17}$
$8 \cdot 15 \equiv 1 \pmod{17}$
$10 \cdot 12 \equiv 1 \pmod{17}$
$14 \cdot 11 \equiv 1 \pmod{17}$

$$\Rightarrow 2 \cdot 3 \cdots 15 = (2 \cdot 9)(3 \cdot 6)(4 \cdot 13)(5 \cdot 7)(8 \cdot 15)(10 \cdot 12)(14 \cdot 11) \equiv 1 \pmod{17}$$

$$\Rightarrow 16(15!) \equiv 16 \pmod{17}$$

$$\Rightarrow 16! \equiv -1 \pmod{17}$$

② What is the remainder when $18!$ is divided by 437?

Soln. $437 = 19 \times 23$

Suppose x is the remainder. Then $437 \mid 18! - x$

$\Rightarrow 19 \mid 18! - x$ & $23 \mid 18! - x$

$\Rightarrow x \equiv 18! \pmod{19}$ and $x \equiv 18! \pmod{23}$

By Wilson's Thm., $18! \equiv -1 \pmod{19}$ and $22! \equiv -1 \pmod{23}$

$$-1 \equiv 22! \equiv 18! \times 19 \times 20 \times 21 \times 22$$
$$\equiv 18! (-4)(-3)(-2)(-1)$$
$$\equiv 18! (24)$$
$$\equiv 18! \pmod{23}$$

i.e. $19 \mid 18! + 1$ & $23 \mid 18! + 1$

Since $\gcd(19, 23) = 1$, $437 \mid 18! + 1$

i.e. $18! \equiv -1 \pmod{437}$

∴ remainder when $18!$ is divided by 437 is 436.

③ Show $4(29!)+5!$ is divisible by 31

Soln. $30! \equiv -1 \pmod{31}$ by Wilson's Thm

Also, $30 \equiv -1 \pmod{31}$

$\Rightarrow 29! \equiv 1 \pmod{31}$

Hence, $4(29!)+5! \equiv 4(1)+5! \equiv 124 \equiv 0 \pmod{31}$

④ For any odd prime p,

$$1^2 \cdot 3^2 \cdot 5^2 \cdots (p-2)^2 \equiv (-1)^{\frac{p+1}{2}} \pmod{p}$$

Soln modulo p

Note that $1 \equiv -(p-1)$, $2 \equiv -(p-2)$, $4 \equiv -(p-4)$, $6 \equiv -(p-6)$, ..., $p-5 \equiv -5$, $p-3 \equiv -3$, $p-1 \equiv -1$.

Multiply all these congruences to get

$$2 \cdot 4 \cdot 6 \cdots (p-1) \equiv (-1)^{\frac{p-1}{2}} 1 \cdot 3 \cdot 5 \cdots (p-2)$$

$$\Rightarrow (p-1)! = (2 \cdot 4 \cdot 6 \cdots (p-1))(1 \cdot 3 \cdot 5 \cdots (p-2))$$
$$= (-1)^{\frac{p-1}{2}} (1 \cdot 3 \cdot 5 \cdots (p-2))(1 \cdot 3 \cdot 5 \cdots (p-2))$$
$$= (-1)^{\frac{p-1}{2}} 1^2 \cdot 3^2 \cdot 5^2 \cdots (p-2)^2$$

By Wilson's Thm, $(p-1)! \equiv -1 \pmod{p}$

$$\Rightarrow (-1)^{\frac{p-1}{2}} 1^2 3^2 5^2 \cdots (p-2)^2 \equiv -1 \pmod{p}$$

$$\Leftrightarrow 1^2 3^2 5^2 \cdots (p-2)^2 \equiv (-1)^{\frac{p+1}{2}} \pmod{p}$$

by multiplying both sides by $(-1)^{\frac{p-1}{2}}$

⑤ Read the statement of Theorem 5.5 (we will do the proof in class next time)

Note that Theorem 5.5 gives the claim we needed to finish the proof that "there are infinitely many primes of form $4k+1$"

claim All odd prime divisors of a^2+1 are of the form $4k+1$

Pf: If $p \mid a^2+1$ then the congruence $x^2+1 \equiv 0 \pmod{p}$ has a solution. From Theorem 5.5, $p \equiv 1 \pmod{4}$.

[Make sure you understand the direct proof using Fermat's Thm]