Recall : (Fermat's Theorem) $a \not\equiv 0 \pmod p \Rightarrow a^{p-1} \equiv 1 \pmod p$

- $x^{p-1}-1$ and $(x-1)(x-2)\cdot\ldots\cdot(x-(p-1))$ have the same coefficients in mod p

- $a^p \equiv a \pmod p$ for all a.

- $x^p - x$ and $x(x-1)(x-2)\cdot\ldots\cdot(x-(p-1))$ have the same coefficients in mod p.

1. Compute $2^{1003} \pmod{11}$

2. Prove $30 \mid n^{25} - n$

3. Solve $x^{17} + 6x^{14} + 2x^5 + 1 \equiv 0 \pmod 5$

We continue with some applications of Fermat's Theorem.

4. Wilson's Theorem: $n \geqslant 2$ is a prime if and only if $(n-1)! \equiv -1 \pmod n$

If n is not a prime, then $n = ab$ for some $2 \leqslant a, b \leqslant n-1$.

$\Rightarrow (n-1)!$ is divisible by $a \Rightarrow (n-1)! \equiv 0 \pmod a$

However $(n-1)! \equiv -1 \pmod n$ will require $(n-1)! \equiv -1 \pmod a$, not possible.

If n is a prime, then by Fermat's Theorem we have $x^{n-1} - 1 \equiv (x-1)(x-2) \cdot \ldots (x-(n-1)) \pmod{n}$

Plugging $x=0$ in, we get

$$-1 \equiv (-1) \cdot (-2) \cdot \ldots (-(n-1)) \pmod{n}$$

$$-1 \equiv (-1)^{n-1} \cdot (n-1)! \pmod{n}$$

$$-1 \equiv (n-1)! \pmod{n}$$

because $n-1$ is even or $n=2$.

(5) <u>Theorem:</u> p odd prime. $x^2 + 1 \equiv 0 \pmod{p}$ has a solution if and only if $p \equiv 1 \pmod{4}$.

If $x^2 + 1 \equiv 0 \pmod{p} \Rightarrow x^2 \equiv -1 \pmod{p}$

$$\Rightarrow (x^2)^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}} \pmod{p}$$

$$\Rightarrow x^{p-1} \equiv (-1)^{\frac{p-1}{2}} \pmod{p}$$

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

$$\Rightarrow \frac{p-1}{2} = 2k \text{ is even}$$

$$\Rightarrow p = 4k+1.$$

If $p \equiv 1 \pmod 4$, then we write $p = 4k+1$.

Choose $x = (2k)! = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot 2k$, then

$$x^2 \equiv (1 \cdot 2 \cdot 3 \cdot \ldots 2k) \cdot (1 \cdot 2 \cdot 3 \cdot \ldots \cdot 2k)$$

$$\equiv (1 \cdot 2 \cdot 3 \cdot \ldots \cdot 2k) \cdot \left(-4k \cdot -(4k-1) \cdot -(4k-2) \cdot \ldots \cdot -(2k+1)\right)$$

$$\equiv (1 \cdot 2 \cdot 3 \cdot \ldots 2k) \cdot ((2k+1) \cdot \ldots \cdot 4k) \cdot (-1)^{2k}$$

$$\equiv (4k)! \longrightarrow (p-1)!$$

$$\equiv -1 \pmod p$$

To test whether n is a prime or not, Wilson's Theorem can be used

- $(n-1)! \not\equiv -1 \pmod n \Rightarrow n$ is not prime.

  not easy to compute

On the other hand, computing powers mod n is much easier:

(Successive squaring method)

Compute $11^{42} \pmod{53}$

$11^{42} = 11^{32} \cdot 11^{8} \cdot 11^{2}$

$11^{1} \equiv 11 \pmod{53}$, $11^{2} \equiv 15 \pmod{53}$, $11^{4} \equiv 13 \pmod{53}$

$11^{8} \equiv 10 \pmod{53}$, $11^{16} \equiv -6 \pmod{53}$, $11^{32} \equiv 36 \pmod{53}$

$\Rightarrow 11^{42} \equiv 36 \cdot 10 \cdot 15 \equiv (-11) \cdot 15 \equiv -6 \pmod{53}$

Can we use Fermat's Theorem $a^{p} \equiv a \pmod{p}$ for primality testing?

- If $a^{n} \not\equiv a \pmod{n} \Rightarrow n$ is not prime.
- Can we say n is not prime $\Rightarrow a^{n} \not\equiv a \pmod{p}$?

  Answer is "No".

Let's say "n passes the base a test" if $a^{n} \equiv a \pmod{n}$.

Smallest value of a to try is $a = 2$.

Question: Is there any composite number n which passes the base 2 test?

Yes and we'll call such numbers pseudoprimes.

- $341 = 11 \cdot 31$ is a pseudoprime:

To prove $2^{341} \equiv 2 \pmod{341}$

- $2^{341} \equiv (2^{10})^{34} \cdot 2 \equiv 1^{34} \cdot 2 \equiv 2 \pmod{11}$
- $2^{341} \equiv (2^{30})^{11} \cdot 2^{11} \equiv 1^{11} \cdot 2^{11} \equiv 2 \pmod{31}$

$$\downarrow$$

$$2^5 \cdot 2^5 \cdot 2 \equiv 2 \pmod{31}$$

Theorem: There are infinitely many pseudoprimes

Proof: n pseudoprime $\Rightarrow 2^n - 1$ is also pseudoprime

Exercise

(Textbook Theorem 4.7.)