Last class: $(x+y)^p \equiv x^p + y^p \pmod p$ only if p is prime.

Theorem. Fermat's Little Theorem.
If $n \in \mathbb{Z}$, p prime then $n^p \equiv n \pmod p$.
Further, if $n \not\equiv 0 \pmod p$ then $n^{p-1} \equiv 1 \pmod p$.

proof.
First, prove 'further...'.
If $n^p \equiv n \pmod p$ and $n \not\equiv 0 \pmod p$ then $\gcd(n,p) = 1$.
So $[n]$ invertible in $\mathbb{Z}/p\mathbb{Z}$.
So there exists $m \in \mathbb{Z}$ so that $nm \equiv 1 \pmod p$.
Then,

$$n^p m \equiv nm \pmod p$$
$$n^{p-1} nm \equiv 1$$
$$n^{p-1} \equiv 1$$

Note: $p \geq 2$ so $p-1 \geq 1$)
Next, prove $n^p \equiv n \pmod p$ by induction on n for $n \geq 0$.
(i) For $n = 0$, $0^p \equiv 0 \pmod p$.
(ii) Let $n \geq 0$. Assume $n^p \equiv n \pmod p$.
Then,

$$(n+1)^p \equiv n^p + 1^p \pmod p \quad \text{(by Lemma)}$$
$$\equiv n + 1 \quad (n^p \equiv n \text{ by IA}).$$ □

Exercise.
Complete proof by induction for $n < 0$. ($n \in \mathbb{Z}$, must prove both)
Hint: $n = -m$, $m > 0$. Use previous case.

Application: Computing Large Powers mod p.

ex. Compute $25^{134} \pmod{11}$.
11 prime, so $x^{10} \equiv 1 \pmod{11}$, $x \not\equiv 0$.
So

$$25^{134} \equiv 3^{134} \quad (25 = 2 \cdot 11 + 3)$$
$$\equiv (3^{10})^{13} 3^4$$
$$\equiv 1^{13} 3^4 \quad \text{by Fermat}$$
$$\equiv 9^2 \quad (3^4 = (3^2)^2 = 9^2)$$
$$\equiv (-2)^2 \quad (-2 = -1 \cdot 11 + 9)$$
$$\equiv 4 \pmod{11}$$

ex. Compute $25^{134} \pmod{14}$.
14 not prime. Can't use Fermat. Use repeated squaring.
First, $25 \equiv -3$ (since $25 \equiv 11$ and $-3 = -1 \cdot 14 + 11$)

$$(-3)^2 \equiv 9 \equiv -5$$
$$(-3)^4 \equiv ((-3)^2)^2 \equiv 9^2 \equiv (-5)^2 \equiv 25 \equiv -3$$
$$(-3)^8 \equiv ((-3)^4)^2 \equiv (-3)^2 \equiv -5$$
$$(-3)^{16} \equiv -3$$
$$(-3)^{32} \equiv -5$$
$$(-3)^{64} \equiv -3$$
$$(-3)^{128} \equiv -5.$$

Then $25^{134} \equiv (-3)^{128+4+2}$
$\equiv (-3)^{128}(-3)^4(-3)^2 \equiv (-5)(-3)(-5) \equiv (-3)^2 \equiv 9 \pmod{14}$.

Application: Fermat's Primality Test

Given $n \in \mathbb{N}$, how to check if n is prime?
Simple test: Compute n/k, $k = 2, 3, 4, 5, \cdots$
If get remainder 0, then $k|n$ so n is not prime.
If all remainders $\neq 0$, n prime.
You only need to check up to $k = \lfloor \sqrt{n} \rfloor$ since $n = ab$ then $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$. Very inefficient.

Fermat's (Non-) Primality Test
Idea: If n prime, then $a^{n-1} \equiv 1 \pmod{n}$ (for $a \not\equiv 0 \bmod n$).
Hence if $a^{n-1} \not\equiv 1$, n is not prime.
Algorithm:
(1) Choose at random $2 \leq a < n$ (so $a \not\equiv 0 \bmod n$).
(2) Compute $a^{n-1} \pmod{n}$. Use repeated squaring.
(3) If $a^{n-1} \not\equiv 1$, n not prime.
(4) If $a^{n-1} \equiv 1$, n might be prime.
(5) If (4), repeat test.
If repeat with "n might be prime" many times, n has high probability of being prime.

ex. Test $n = 9$. Choose $a = 2$.
Compute $2^8 \equiv 4^4 \equiv 16^2 \pmod{9}$
$\equiv (-2)^2 \equiv 4 \not\equiv 1$
So 9 not prime.

ex. Test $n = 11$
$a = 2$: $2^{10} \equiv 4^5 \equiv (4^2)^2\, 4 \equiv 16^2\, 4 \equiv 5^2 4 \equiv 100 \equiv 1 \pmod{11}$
$a = 3$: $3^{10} \equiv 1 \pmod{11}$
So 11 (might be) prime.

ex. Try $n = 341$. $(341 = 11 \cdot 31)$
$a = 2$: $2^{340} \equiv \cdots \equiv 1 \pmod{341}$
$a = 3$: $3^{340} \equiv 1$
$a = 8$: $8^{340} \equiv 1$
341 is called a Fermat pseudo-prime to bases 2, 3, 8.

Cryptography & RSA

Problem.
Ann and Bert want to communicate over a public channel, such that if the messages are intercepted, they cannot be understood.
Define a message M as a binary string.

Auson Li

Vernam One-Time Pad

(1) Ann and Bert meet in person and generate a long sequence P of random bits.

(2) Ann, Bert separate. Each take copy of P.

(3) Bert wants to send message to Ann.
Say $m = 01101$.
Bert looks up first 5 bits of P, add to m mod 2. Bitwise, no carries. Say $P = 11010$.

$$\begin{array}{rl} m = & 0\,1\,1\,0\,1 \\ P = & 1\,1\,0\,1\,0 \\ \hline \bar{m} & 1\,0\,1\,1\,1 \end{array} \leftarrow \text{encrypted message.}$$

Bert sends $\bar{m}$ to Ann.

(4) Ann receives $\bar{m}$. To decode, take first 5 bits of P and add.

$$\begin{array}{rl} \bar{m} = & 1\,0\,1\,1\,1 \\ P = & 1\,1\,0\,1\,0 \\ \hline m = & 0\,1\,1\,0\,1 \end{array}$$

Ann will obtain m since P is added twice to m.

$$\bar{m} \left\{ \begin{array}{rl} m = & 0\,1\,1\,0\,1 \\ P = & 1\,1\,0\,1\,0 \\ P = & 1\,1\,0\,1\,0 \\ \hline m = & 0\,1\,1\,0\,1 \end{array} \right. \quad P+P = 00000$$

(5) To reply, Ann uses next bits in P. Bert uses some bits to decode.

Comments:

(1) Perfectly secure if P not obtained.

(2) Not secure if you reuse any bits of P.

(3) Once you run out of bits of P, need to meet again for new P.

RSA Scheme

(1) Ann creates two large primes p, q (100 or more digits).
(How? Create a number of 100 digits at random; run a primality test. If not prime, repeat. For numbers of 100 digits, probability of being prime $\approx 10\%$).
Then, find k (public key) such that $\gcd(k, (p-1)(q-1)) = 1$.
(How? Choose k at random, find gcd via Euclid. If not 1, try again).
Find $[k]^{-1} = [s]$ in $\mathbb{Z}/(p-1)\mathbb{Z}$.
(again, by Euclid). s called secret key.

(2) Let $n = pq$. Ann makes n, k publicly known (wants to receive messages from anybody).

(3) Bert wants to send message m (binary string). Think of m as an integer. (Restriction: $m < n$).
Compute $\bar{m} = m^k \pmod n$, i.e. $0 \leq \bar{m} < n$).
Sends $\bar{m}$ to Ann.

(4) Ann receives $\bar{m}$. To decipher, compute $\bar{m}^s \pmod n$.
This will be m.