Modular Arithmetic

$a \bmod b$ = remainder when a is divided by b

$13 \bmod 4 = 1$

$27 \bmod 3 = 0$

$2 \bmod 4 = 2$

$3^1 \to 3$

$3^2 \to 9$

$3^3 \to 7$

$3^4 \to 1$

$3^5 \to 3$

$3^6 \to 9$

$3^{202} \to 3^{202 \bmod 4} \to 3^2 \to 9$

$9 \bmod 4 = 1$

$17 \bmod 4 = 1$

$\Rightarrow 9 \bmod 4 = 17 \bmod 4 = 1$

$9 \equiv 17 \pmod 4$

$a \bmod m = b \bmod m \iff a \equiv b \pmod m \iff m \mid a-b$

$a \bmod m = r \iff a = m \cdot q + r$

$13 \bmod 4 = 1$

$13 = 4 \cdot 3 + 1$

$$4\overline{)13}\ \ 3\ R1$$

$a \equiv b \pmod m$

$b \equiv c \pmod m$

$a \bmod m = b \bmod m$

$b \bmod m = c \bmod m$

$a \bmod m = c \bmod m$

$\Rightarrow a \equiv c \pmod m$

$a \equiv b \pmod m$ $\quad a \bmod m = b \bmod m$

$c \equiv d \pmod m$ $\quad c \bmod m = d \bmod m$

$a+c \equiv b+d \pmod m$ $\quad (a \bmod m + c \bmod m) = (b \bmod m + d \bmod m)$

$a-c \equiv b-d \pmod m$ $\quad (a+c) \bmod m = (b+d) \bmod m$

$ac \equiv bd \pmod m$

$a \equiv b \pmod m$

$a \bmod m = b \bmod m = r$

$a = mq_a + r$

$b = mq_b + r$

$a-b = m(q_a - q_b)$

$m \mid a-b$

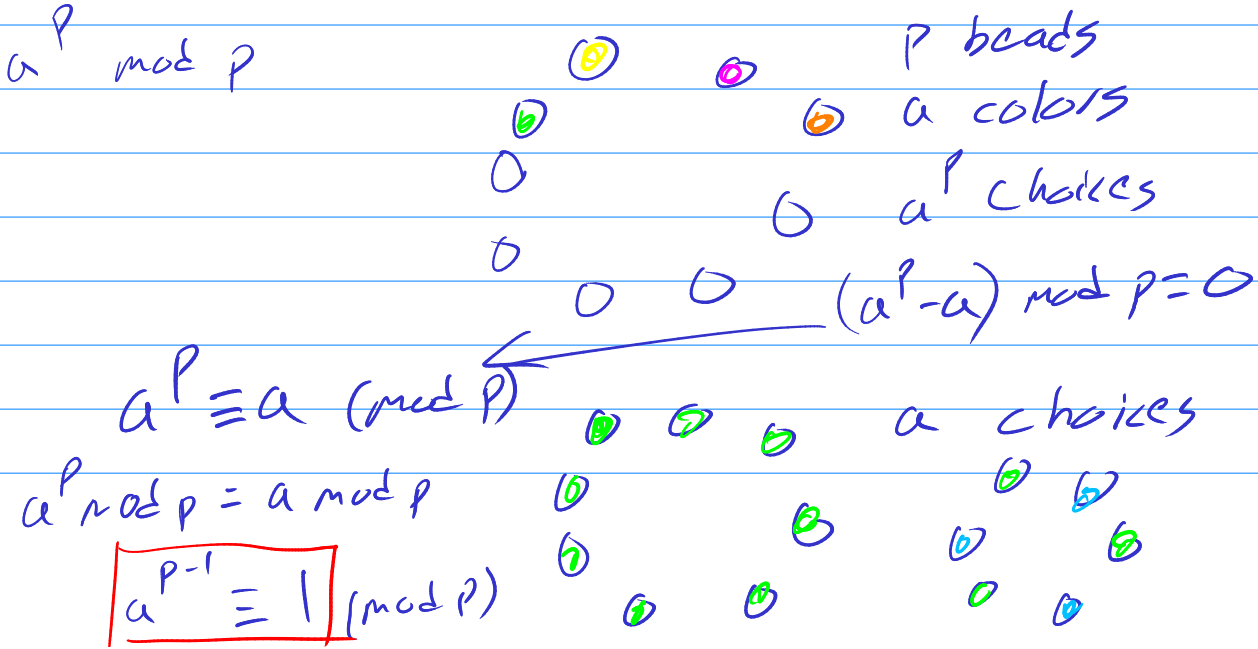
what is $-1 \bmod 4 = (-1+4) \bmod 4 = 3$

$-1 \bmod m = m-1$

$-2 \bmod m = m-2$

Fermat's Little Theorem

$a^p \bmod p$



$a^p \equiv a \pmod p$

$a^p \bmod p = a \bmod p$

$\boxed{a^{p-1} \equiv 1 \pmod p}$

$21^{100} \pmod{11} = 1$

$21^{10} \equiv 1 \pmod{p}$

$(21^{10})^{10} \equiv 1^{10} \equiv 1 \pmod{11}$