The Modular Arithmetic Formula Sheet
Primer

$N, d, q, r \in \mathbb{Z}, \quad (0 \le r < d)$

$N = dq + r$

Addition / Subtraction

$a \equiv b \pmod{m}, \quad c \equiv d \pmod{m} \Rightarrow$

$a \pm c \equiv b \pm d \mod m$

Multiplication

$a \equiv b \pmod{m}, \quad c \equiv d \pmod{m} \Rightarrow$

$ac \equiv bd \pmod{m}$

Exponent

$a \equiv b \pmod{m}, \quad k \in \mathbb{Z}^+ \Rightarrow$

$a^k \equiv b^k \pmod{m}$

Division

$a \equiv b \pmod{m}, \quad k \in \mathbb{Z}_\phi$

$\frac{a}{k} \equiv \frac{b}{k} \left(\mod \frac{m}{(m,k)}\right)$

GCD

Hints: Power of $(-1)^x$

Continuous Simplification

Eulers Totient Function

$$\phi(N) = N * \prod_{i=1}^{k} (1 - 1/P_i)$$ — P - Primes

$$\phi(P^k) = P^{k-1}(P-1)$$

Positive One via Eulers Theorem

$$a^{\phi(N)} \equiv 1 \pmod{N}$$

Modular Inverse

$$X \cdot Y \equiv 1 \pmod{m}$$

$$Y \equiv X^{-1} \pmod{m}$$

$$Y \equiv 1/x \pmod{m}$$

Exists only if x, m are relative prime

Computing modular Inverse

$$a^{-1} = a^{\phi(m)-1} \pmod{m}$$

a and m relative prime

Wilson's Theorem

$$(P-1)! \equiv -1 \pmod{p}$$

Euler's Theorem

$$a^{\phi(n)} \equiv 1 \pmod{n}$$ n and a are relative prime

Fermat's Little Theorem

$$a^{p-1} \equiv 1 \pmod{p}$$ P, a relative prime

$$a^{p} \equiv a \pmod{p}$$