Some useful facts about primes, divisibility and modular arithmetic:

Terminology: An integer is **prime** it is has exactly two positive divisors (in particular, 1 is not prime). An integer a **divides** another integer b iff there exists an integer k so that $ak = b$.

Primes and divisibility: If p divides ab then either p divides a or p divides b (perhaps both). Every integer can be written as the product of primes: $n = p_1^{e_1} \cdots p_r^{e_r}$ (the fundamental theorem of arithmetic.

How many primes are there?: There are infinitely many primes.

Equivalence mod n: We say a is congruent to b modulo n if there exists an integer k so that $a = nk + b$. We write $a \equiv b \pmod{n}$. E.g., $3 \equiv 20 \equiv -31 \pmod{17}$.

Modular arithmetic: $(a \pm b) \pmod{n} \equiv a \pmod{n} \pm hb \pmod{n}$, same for multiplication. Division doesn't always work.

GCD: Division by $a \pmod{n}$ is multiplying by its reciprocal so we ask the question when does $a \pmod{n}$ have an reciprocal? I.e., when can you solve $ax \equiv 1 \pmod{n}$? E.g., $3x \equiv 1 \pmod{7}$, means $x \equiv 5 \pmod{7}$. E.g., $4x \equiv 2 \pmod{6}$. Can't do it. In general if $\gcd(a, n) = 1$, you can solve $ax \equiv n \pmod{n}$.

XGCD: How do you solve it? The $\gcd(a, b) = d$ is the same as: there exist two numbers x and y so that $ax + by = d$. If $\gcd(a, n) = 1$, then there are two numbers x and y so that $ax + ny = 1$, i.e., $ax \equiv 1 \pmod{n}$. How do you find x and y? Answer: extended Euclidean algorithm: find x, y so that $101x + 64y = 1$.