Math 310
Handy facts for the first exam

Induction. Three different equivalent versions:

1. (Well-orderedness) Every non-empty set of natural numbers has a smallest element.
2. (Induction) *If* $P(n)$ is a statement about the integer n and
   (a) $P(n_0)$ is true for some integer n_0, and
   (b) if $P(n-1)$ is true, then $P(n)$ is true,
   then $P(n)$ is true for every integer $n \geq n_0$
3. (Complete Induction) *If* $P(n)$ is a statement about the integer n and
   (a) $P(n_0)$ is true for some integer n_0, and
   (b) if $P(k)$ is true for every $n_0 \leq k < n$, then $P(n)$ is true,
   then $P(n)$ is true for every integer $n \geq n_0$

An integer p is *prime* if whenever $p = ab$ with $a, b \in \mathbb{Z}$, either $a = \pm n$ or $b = \pm n$.

[For sanity's sake, we will take the position that primes should <u>also</u> be ≥ 2 .]

There are infinitely many distinct primes.

Every integer $n \geq 2$ can be expressed as a product of primes; $n = p_1 \cdot \cdots \cdot p_k$.

If we insist that the primes are written in increasing order, $p_1 \leq \ldots \leq p_k$, then this representation is *unique.*

Exponential notation: any $n \geq 2$ can be uniquely expressed as $n = p_1^{\alpha_1} \cdot \cdots \cdot p_r^{\alpha_r}$ with $\alpha_i \geq 1$ for each i and $p_1 < \ldots < p_r$.

The Division Algorithm: For any integers $n \geq 0$ and $m > 0$, there are *unique* integers q and r with $n = mq + r$ and $0 \leq r \leq m - 1$.

[Note: this is also true for any integers n, m with $m \neq 0$, although you need to replace "$m - 1$" with "$|m - 1|$" .]

The basic idea: keep repeatedly subtracting m from n until what's left is less than m.

Notation: $b|a$ = "b divides a" = "b is a divisor of a" = "a is a multiple of b", means $a = bk$ for some integer k .

If $b|a$ and $a \neq 0$, then $|b| \leq |a|$.

If $a|b$ and $b|c$, then $a|c$

If $a|c$ and $b|d$, then $ab|cd$

If p is prime and $p|ab$, then either $p|a$ or $p|b$

Notation: $(a, b) = \gcd(a, b)$ = greatest common divisor of a and b

Different, equivalent, formulations for $d = (a, b)$:

(1) $d|a$ and $d|b$, and if $c|a$ and $c|b$, then $c \leq d$.

(2) d is the smallest *positive* number that can be written as $d = ax + by$ with $a, b \in \mathbb{Z}$.

(3) $d|a$ and $d|b$, and if $c|a$ and $c|b$, then $c|d$.

(4) d is the *only* divisor of a and b that can be expressed as $d = ax + by$ with $a, b \in \mathbb{Z}$.

If $c|a$ and $c|b$, then $c|(a, b)$

If $c|ab$ and $(c, a) = 1$, then $c|b$

If $a|c$ and $b|c$, and $(a, b) = 1$, then $ab|c$

If $a = bq + r$, then $(a, b) = (b, r)$

Euclidean Algorithm: This last fact gives us a way to compute (a,b), using the division algorithm:

Starting with $a > b$, compute $a = bq_1 + r_1$, so $(a, b) = (b, r_1)$. Then compute $b = r_1 q_2 + r_2$, and repeat: $r_{i-1} = r_i q_{i+1} + r_{i+1}$. Continue until $r_{n+1} = 0$, then $(a, b) = (b, r_1) = (r_1, r_2) = \ldots = (r_n, r_{n+1}) = (r_n, 0) = r_n$.

Since $b > r_1 > r_2 > r_3 > \ldots$, this process must end, by well-orderedness.

We can reverse these calculations to recover $(a,b) = ax+by$, by rewriting each equation in our algorithm as $r_{i+1} = r_{i-1} - r_i q_{i+1}$, and then repeatedly substituting the higher equations into the lowest one, in turn, working up through the list of equations.

Primality Testing:

If $n \geq 2$ is not prime, then it has a prime factor $p \leq \sqrt{n}$. So to test if a number n is prime, 'just' check to see if $p|n$ for any prime $p \leq \sqrt{n}$.

The Sieve of Eratosthenes: To find all primes between 2 and n, first make a list, then repeat the following procedure: circle the smallest number p not already either circled or crossed off, then cross off all other multiples of p. Continue until the number you are about to circle is larger than $\sqrt{n}$. Then every number either circled or *not crossed off* is prime, while every number crossed off is *not* prime.

Congruence modulo n **:** Notation: $a \equiv b \pmod{n}$ (also written $a \underset{n}{\equiv} b$) means $n|(b-a)$

Equivalently: the division algorithm will give the same remainder for a and b when you divide by n

Congruence mod n is an *equivalence relation*, which means

(Reflexive) $a \underset{n}{\equiv} a$ for every $a \in \mathbb{Z}$

(Symmetric) If $a \underset{n}{\equiv} b$, then $b \underset{n}{\equiv} a$

(Transitive) If $a \underset{n}{\equiv} b$ and $b \underset{n}{\equiv} c$, then $a \underset{n}{\equiv} c$

If $a = b$, then $a \underset{n}{\equiv} b$ for any $n \in \mathbb{Z}$

If $a \underset{n}{\equiv} b$ and $k \in \mathbb{Z}$, then $ka \underset{n}{\equiv} kb$

If $a \underset{n}{\equiv} b$ and $m|n$, then $a \underset{m}{\equiv} b$

(*) If $a \underset{n}{\equiv} b$ and $c \underset{n}{\equiv} d$, then $a+c \underset{n}{\equiv} b+d$ and $ac \underset{n}{\equiv} bd$

The *congruence class* of a mod n is the collection of all integers congruent mod n to a:

$[a]_n = \{b \in \mathbb{Z} : a \underset{n}{\equiv} b\} = \{b \in \mathbb{Z} : n|(b-a)\}$

Because $\underset{n}{\equiv}$ is an equivalnce relation, these sets are either *disjoint* or *equal*. And because every integer is congruent mod n to its remainder on division by n, there are exactly n congruence classes mod n, which can be represented as $[0]_n, [1]_n, \dots, [n-1]_n$. The set of these n equivalence classes is denoted $\mathbb{Z}/n\mathbb{Z}$ or $\mathbb{Z}_n$, and is called the *integers mod n*

(*) tells us that it *makes sense* to add and multiply congruence classes:

$[a]_n + [b]_n = [a+b]_n \quad , \quad [a]_n \cdot [b]_n = [ab]_n$

These facts can be used to carry out some otherwise fairly difficult calculations very quickly:

To compute $[a^m]_n$, we note that $[a^m]_n = [a]_n^m$, so we first write $a = nq+r$, so $[a^m]_n = [a]_n^m = [r]_n^m$. Then we look at the list $[r]_n^1, [r]_n^2, [r]_n^3, [r]_n^4, \dots$, and continue until the power equals $[0]_n, [1]_n$ or it repeates itself. All of these can be used to reduce m. For example,

$[107^{1015}]_7$: $[107]_7 = [7 \cdot 15 + 2]_7 = [2]_7$, and $[2]_7^3 = [8]_7 = [1]_7$, so since $1015 = 3 \cdot 338 + 1$, we have $[107^{1015}]_7 = [2]_7^{1015} = [2]_7^{3 \cdot 338+1} = ([2]_7^3)^{338} \cdot [2]_7^1 = [1]_7^{338} \cdot [2]_7 = [2]_7$.

We can show that some equations have no integer solutions by showing that the 'same' equations have no solutions in some $\mathbb{Z}_n$ (coefficients need to be interpreted as being <u>in</u> $\mathbb{Z}_n$ ...). The latter is far less difficult to do, in general, because $\mathbb{Z}_n$ has only n elements! For example,

In $\mathbb{Z}_5$, $0^2 = 0$, $1^2 = 1$, $2^2 = 4$, $3^2 = 4$, and $4^2 = 1$, and so $x^2 = [3]_5$ has no solution in $\mathbb{Z}_5$. So the equation

$$x^2 - 5y^2 = 531253$$

has no solution with $x, y \in \mathbb{Z}$, since if it did, then

$[x^2 - 5y^2]_5 = [x]_5^2 - [5]_5 \cdot [y]_5^3 = [x]_5^2 - [0]_5 \cdot [y^3]_5 = [x]_5^2 = [531253]_5 = [3]_5$

so $[x]_5^2 = [3]_5$, which we know is impossible!