Putnam preparation

Number Theory and Congruences

In the presentation of this introduction we follow O. Holtz's and C. Muscalu's notes. As usual, all the problems are from outside sources, I make no claim of originality on my part.

Basic notation: $\mathbb{N}$ denotes the set of natural numbers $\{1, 2, 3, ...\}$ and $\mathbb{Z}$ denotes the set of all integers $\{..., -2, -1, 0, 1, 2, 3, ...\}$.

Definitions: Given two integers a, b, we say that a divides b, and we write $a|b$, if $b = ac$ for some integer c. Then a is a divisor, or factor of b. A natural number $p > 1$ is prime if 1 and p are its only positive divisors. A natural number $n > 1$ that is not prime is said to be composite.

Theorem (Euclid): There are infinitely many prime numbers.

More Definitions: If a and b are integers that are not both zero, their greatest common divisor, denoted by (a, b) or $gcd(a, b)$ is the largest natural number that divides both a and b. If $(a, b) = 1$, then a and b are said to be relatively prime.

The least common multiple of a and b, denoted by $lcm(a, b)$, is the smallest natural number that is divisible by both a and b.

The notions of greatest common divisor and least common multiple generalize to finite collections of integers.

Division algorithm: If a and b are arbitrary integers, $b > 0$, there are unique integers q and r such that

$$a = qb + r; \quad 0 \leq r < b \ .$$

Then $(a, b) = (b, r)$.

Corollary 1: Given positive integers a and b, there are integers s and t such that

$$sa + tb = (a, b)$$

Corollary 2: Given positive integers a, b, and c, there are integers s and t such that

$$sa + tb = c$$

if and only if (a, b) divides c. In particular, there are integers s and t such that $sa + tb = 1$ if and only if $(a, b) = 1$.

Euclid's lemma. If $a|bc$ and $(a, b) = 1$, then $a|c$.

Fundamental theorem of arithmetic (unique factorization). Every natural number $n > 1$ can be written uniquely, up to the order of factors, as the product of primes. I.e. every natural number $n > 1$ can be written in one and only one way (disregarding the order of factors) in the form

$$n = p_1^{\alpha_1} p_2^{\alpha_2} ... p_k^{\alpha_k}$$

where $p_1, p_2, ..., p_k$ are different prime numbers and $\alpha_1, \alpha_2, ..., \alpha_k$ are positive integers.

As a consequence, all the divisors of

$$n = p_1^{\alpha_1} p_2^{\alpha_2} ... p_k^{\alpha_k}$$

are of the form

$$m = p_1^{\beta_1} p_2^{\beta_2} ... p_k^{\beta_k}, \qquad 0 \leq \beta_i \leq \alpha_i, \qquad i = 1, 2, ..., k,$$

and every such number is a divisor of n. Thus, n has exactly $(\alpha_1 + 1)(\alpha_2 + 1)...(\alpha_k + 1)$ distinct divisors.

Another easy consequence of unique factorization is that an integer $n = p_1^{\alpha_1} p_2^{\alpha_2} ... p_k^{\alpha_k}$ is a perfect square if and only if all α_i are even, a perfect cube if and only if all α_i are multiples of 3, and so on.

A further consequence of unique factorization: consider $a, b, ..., g$ a finite number of positive integers. Suppose their unique factorizations are

$$a = p_1^{a_1} p_2^{a_2} ... p_k^{a_k}, \quad b = p_1^{b_1} p_2^{b_2} ... p_k^{b_k}, \quad \ldots, \quad g = p_1^{g_1} p_2^{g_2} ... p_k^{g_k},$$

where $a_1, \ldots, a_k, b_1, \ldots, b_k, \ldots, g_1, \ldots, g_k$ are nonnegative integers (some may be zero). Then

$$gcd(a, b, \ldots, g) = p_1^{m_1} p_2^{m_2} ... p_k^{m_k},$$

and

$$lcm(a, b, \ldots, g) = p_1^{M_1} p_2^{M_2} ... p_k^{M_k},$$

where $m_i = \min\{a_i, b_i, \ldots, g_i\}$, and $M_i = \max\{a_i, b_i, \ldots, g_i\}$ for each $i = 1, 2, \ldots, k$.

From this it easily follows that

$$gcd(a, b)\ lcm(a, b) = ab.$$

Modular arithmetic or congruences. Let a and b be integers and n be a natural number. Then a is congruent to b modulo n, written as

$$a \equiv b\ (mod\ n)$$

if $n|(a - b)$.

The number n is called the modulus of the congruence. Congruence modulo n divides the set $\mathbb{Z}$ into n subsets called residue classes. E.g. if $n = 2$, then the two residue classes are the even integers and the odd integers. The integers a and b are in the same residue class if and only if $a \equiv b\ (mod\ n)$.

Basic properties.

- Reflexivity: $a \equiv a\ (mod\ n)$.
- Symmetry: If $a \equiv b\ (mod\ n)$, then $b \equiv a\ (mod\ n)$.
- Transitivity: If $a \equiv b\ (mod\ n)$, and $b \equiv c\ (mod\ n)$, then $a \equiv c\ (mod\ n)$.
- Congruences may be added: If $a \equiv b\ (mod\ n)$, and $c \equiv d\ (mod\ n)$, then $a + c \equiv b + d\ (mod\ n)$.
- Congruences may be multiplied: If $a \equiv b\ (mod\ n)$, and $c \equiv d\ (mod\ n)$, then $ac \equiv bd\ (mod\ n)$.

- Division is not so simple: $6 \equiv 36 \ (mod\ 10)$, but dividing by 2 would give $3 \equiv 18 \ (mod\ 10)$ which is not true! The problem above is that 2 divides 10. We can do two things:
- Divide by a number k relatively prime to n: if $ab \equiv ac \ (mod\ n)$ and $(a, n) = 1$, then $b \equiv c \ (mod\ n)$.
- Divide all three numbers by a number k which is a divisor of n: if $ab \equiv ac \ (mod\ an)$, then $b \equiv c \ (mod\ n)$.
- You can also reduce n alone: $7 \equiv 13 \ (mod\ 6) \Longrightarrow 7 \equiv 13 \ (mod\ 3)$. But this does not work in the opposite direction: $13 \equiv 16 \ (mod\ 3)$ but $13 \equiv 16 \ (mod\ 6)$ is false!

An important concept related to residue classes is that of the field $\mathbb{Z}_p$ of integers mod p, where p is a prime.

Definition: $\mathbb{Z}_n$ is the set $\{0, 1, 2, \ldots, n-1\}$ with addition and multiplication mod n.

Facts: $\mathbb{Z}_n$ is a ring with addition and multiplication modulo n, i.e. addition and multiplication are commutative and associative, the distributive law holds, there exists an element neutral under addition (namely 0), and an element neutral under multiplication (namely 1), and each element has an inverse under addition.

If $n = p$, a prime number, then $\mathbb{Z}_p$ is a finite field, i.e. not only a ring, but also that each element except for 0 has an inverse under multiplication.

Indeed, recall that as a particular case of Corollary 2 above, there are integers s and t such that $sa + tb = 1$ if and only if $(a, b) = 1$. In other words, a has a multiplicative inverse in $\mathbb{Z}_n$ if and only if $(a, b) = 1$. Hence if n is a prime number p, all non-zero numbers $\{1, 2, ..., p-1\}$ have multiplicative inverse and $\mathbb{Z}_p$ is a field.

Fermat's Little Theorem Let a be a positive integer and p be a prime. Then

$$a^p \equiv a \ (mod\ p) \ .$$

The cancellation law tells us that, if $(a, p) = 1$, then we can divide by a above getting

$$a^{p-1} \equiv 1 \ (mod\ p) \ .$$

Euler's Theorem Euler's ϕ function is defined as follows:

$$\phi(m) = \text{ number of elements from } \{1, 2, ..., m\} \text{ that are prime to } m \text{ (including 1).}$$

Then Euler's theorem says

$$(a, m) = 1 \Longrightarrow a^{\phi(m)} \equiv 1 \ (mod\ m).$$

A fact about Euler's ϕ function is that

$$\phi(m) = m \left(1 - \frac{1}{p_1}\right) ... \left(1 - \frac{1}{p_k}\right) \ ,$$

where $m = p_1^{\alpha_1} ... p_k^{\alpha_k}$ is the factorization of m into primes.

Notice that for any positive integers a and n, since there are only finitely many possibilities for the residues of $a^k \ (mod\ n)$, when k is a nonnegative integer, after some time, the residues start to repeat cyclically. E.g. $3^0 \equiv 1 \ (mod\ 8)$, $3^1 \equiv 3 \ (mod\ 8)$, $3^2 \equiv 1 \ (mod\ 8)$, $3^3 \equiv 3^2 \cdot 3 \equiv 1 \cdot 3 \ (mod\ 8)$, $3^4 \equiv 1 \ (mod\ 8)$, and so on. This is useful for finding e.g. the residue of $3^{2700} \ (mod\ 8)$.

Also, when considering, say, squares of integers (or cubes, or fourth powers...), not all possible residues are attained. E.g. $0^2 \equiv 0 \ (mod\ 7)$, $1^2 \equiv 1 \ (mod\ 7)$, $2^2 \equiv 4 \ (mod\ 7)$, $3^2 \equiv 2 \ (mod\ 7)$, $4^2 \equiv (-3)^2 \equiv 2 \ (mod\ 7)$, $5^2 \equiv (-2)^2 \equiv 4 \ (mod\ 7)$, $6^2 \equiv (-1)^2 \equiv 1 \ (mod\ 7)$. This is useful e.g. to show that if $0 \leq a, b \leq 6$ and $a \neq b$, then $a^2 + b^2 \equiv 0 \ (mod\ 7)$ does not have a solution.

Wilson's Theorem The number p is prime if and only if

$$(p-1)! \equiv -1 \ (mod\ p) \ .$$

Chinese remainder theorem Suppose that $n_1, n_2, ..., n_k$ are pairwise relatively prime and $a_1, a_2, ..., a_k$ are arbitrary integers. Then there exist solutions x to the simultaneous congruences

$$x \equiv a_i \ (mod\ n_i) \quad i = 1, ..., k.$$

Any two solutions are congruent modulo $N := n_1 n_2 ... n_k$.

Divisibility criteria When an integer is written in decimal notation (base 10), it is possible to determine very easily if it is divisible by 2 or 5. There are other divisibility tests that are easy to apply. E.g.: An integer N is divisible by 4 if and only if its last two digits are divisible by 4. To see this, write N in base 10:

$$N = (a_n 10^n + \cdots + a_2 10^2) + (a_1 10 + a_0)$$

and note that $a_n 10^n + \cdots + a_2 10^2$ is always divisible by 4. Thus, 4 divides N if and only if 4 divides $(a_1 10 + a_0)$.

One of the most striking and useful divisibility tests is that an integer is divisible by 9 if and only if the sum of its digits (in decimal notation) is divisible by 9. To see why this is so, notice that $10 \equiv 1 \ (mod\ 9)$, and therefore, by the properties of teh modular arithmetic, $10^2 \equiv 1 \ (mod\ 9)$, $10^3 \equiv 1 \ (mod\ 9)$, and so on. It follows that

$$N = a_n 10^n + \cdots + a_2 10^2 + a_1 10 + a_0 \equiv a_n + \cdots + a_2 + a_1 + a_0 \ (mod\ 9).$$

A similar proof shows that an integer is divisible by 3 if and only if the sum of its digits is divisible by 3. As an application of this test, suppose we ask: for what digits x is $4324x98765223$ divisible by 3? We simply need to add the digits modulo 3, and choose x that will make the sum congruent to zero modulo 3. In this case, the sum of the digits is $1 + x$ modulo 3, so the number is divisible by 3 if and only if $x = 2, 5$, or 8.

Another nice divisibility criterion is that of divisibility by 11. The proof follows the lines of the criterion of divisibility by 9, using that $10 \equiv -1 \ (mod\ 11)$. Thus, a number N which in base 10 is written as

$$N = a_n 10^n + \cdots + a_2 10^2 + a_1 10 + a_0 \ ,$$

when divided by 11, has the same remainder as the number $M = a_0 - a_1 + a_2 - a_3 + \cdots + (-1)^n a_n$ when divided by 11.

Based on the fact that $1001 = 7 \times 11 \times 13$, and $1000 \equiv -1 \ (mod\ 1000)$, another divisibility criterion (which is not of very frequent use) can be constructed for either of 7, 11 or 13, namely that a number N which in base 10 is written as

$$N = a_n 10^n + \cdots + a_2 10^2 + a_1 10 + a_0 \ ,$$

when divided by either of the previous numbers (7, 11, 13), has the same remainder as the number $M = (a_2 10^2 + a_1 10 + a_0) - (a_5 10^2 + a_4 10 + a_3) + (a_8 10^2 + a_7 10 + a_6) - \ldots$ when divided by the corresponding number. It is easy to see why it is not of frequent use...

The Greatest Integer Function The greatest integer function associates to a number x the greatest integer less than or equal to x. The standard notation is $\lfloor x \rfloor$. For example, $\lfloor 2 \rfloor = 2$, $\lfloor 1.4 \rfloor = 1$, $\lfloor -2.3 \rfloor = -3$.

Sometimes, the following theorem regarding the greatest integer function is useful.

Beatty's theorem Let α and β be two positive irrational numbers satisfying $\frac{1}{\alpha} + \frac{1}{\beta} = 1$. Then the sequences $\lfloor n\alpha \rfloor$ and $\lfloor n\beta \rfloor$, for $n \geq 1$, are strictly increasing and determine a partition of the set of positive integers into two disjoint sets. In other words, each positive integer shows up in one and only one of the two sequences.

Disclaimer: Most (if not all) the material here is from outside sources, I am not claiming any originality.