Divisibility

Memorize: If a and b are integers, we say that a *divides* b, and write $a|b$, if there is an integer k such that $ak = b$.

Fact D1. Let a, b and c be integers. Then

(i) if $a|b$ and $a|c$, then $a|(b + c)$,

(ii) if $a|b$ then $a|bc$ for all integers c, and

(iii) if $a|b$ and $b|c$ then $a|c$.

You should know how to prove these, and other simple facts about divisibility.

The Division Algorithm. If a and b are integers and $b > 0$, then there exist unique integers q and r so that $a = bq + r$ and $0 \leq r < b$.

The *quotient* q in the division algorithm is equal to $\lfloor \frac{a}{b} \rfloor$ and the *remainder* r is $a (\mathrm{mod}\ b)$ (discussed below).

Prime Numbers

Memorize: An integer $p > 1$ is called *prime* if its only positive divisors are 1 and itself. An integer $n > 1$ which is not prime is called *composite*.

Fundamental Theorem of Arithmetic. Every positive integer can be written as a product of primes in exactly one way, up to the order of the factors.

Fact P1. If n is composite, then n has a (prime) divisor which is between 2 and $\sqrt{n}$.

You should know how to prove the above fact, and also its implications for the Seive of Eratosthenes.

Seive of Eratosthenes. This generates all of the prime numbers less than or equal to n. Start by writing the numbers $2, 3, 4, \ldots, n$ in a line. Then keep repeating the following process until all numbers less than or equal to $\sqrt{n}$ have been crossed out or circled:

REPEAT: Circle the next number which is neither circled nor crossed out, and cross out all other multiples of that number which are in the list (some of these are probably already crossed out).

The numbers which are not crossed out when the process terminates are all of the primes between 2 and n. You should be able to explain why.

The *gcd* and the *lcm*

Memorize: If a and b are integers which are not both zero, the *greatest common divisor* of a and b is the largest integer d such that $d|a$ and $d|b$. It is denoted by $gcd(a, b)$.

Memorize: Integers a and b are called *relatively prime* if $gcd(a, b) = 1$.

Memorize: The *least common multiple* of a and b is the smallest integer m such that $a|m$ and $b|m$. It is denoted by $lcm(a, b)$.

If you know the prime factorizations of the integers a and b, then it is easy to find $gcd(a, b)$ and $lcm(a, b)$. Suppose

$a = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$, where each $e_i \geq 0$, and

$b = p_1^{f_1} p_2^{f_2} \dots p_k^{f_k}$, where each $f_i \geq 0$.

(Notice that the same primes appear in both factorizations, although the exponent may be zero.) Then,

$gcd(a, b) = p_1^{\min\{e_1, f_1\}} p_2^{\min\{e_2, f_2\}} \dots p_k^{\min\{e_k, f_k\}}$, and

$lcm(a, b) = p_1^{\max\{e_1, f_1\}} p_2^{\max\{e_2, f_2\}} \dots p_k^{\max\{e_k, f_k\}}$.

The two equations above imply $gcd(a, b) \times lcm(a, b) = ab$. Thus, for example, if you know $gcd(a, b)$, you can find $lcm(a, b)$ by division.

The reason that the above formulae work comes from Fact D1 (iii) and the Fundamental Theorem of Arithmetic (FTA). Let's look at the *gcd*, the *lcm* is similar. By Fact D1 (iii) any prime divisor of the *gcd* is a divisor of each number, and by the FTA the only primes that divide a number are those that appear in the prime factorization (with a positive exponent). By the FTA again, the highest power of p_i that divides both a and b is the minimum of e_i and f_i. Thus the largest common divisor of a and b is the product of these prime powers.

You should be able to prove the following facts. The second fact below is the underlying reason that the Euclidean Algorithm (for finding $gcd(a, b)$) works.

Fact G1. Suppose x, y, and z are integers. If $x + y = z$ and the integer d divides any two of x, y, and z, then it also divides the third.

Fact G2. If a and b are integers and we use the division algorithm to write $a = bq + r$, then $gcd(a, b) = gcd(b, r)$.

The Euclidean Algorithm. (Given positive integers a and b, find $gcd(a, b)$). Suppose $a \geq b$. Use the division algorithm to write $a = bq + r$, $0 \leq r < b$. If $r = 0$ the *gcd* is b. Otherwise repeat the procedure with b and r in place of a and b (and keep repeating it until you get a remainder of zero).

You should be able to use the Euclidean Algorithm to find the greatest common divisor (and hence the least common multiple) of two integers a and b. You should also be able to explain why the Euclidean Algorithm works.

Let c be an integer. If there exist integers α and β such that $a\alpha + b\beta = c$, then by Fact G1 $gcd(a, b)|c$. Thus any integer which can be written as $a\alpha + b\beta$ (for integers α and β) is a multiple of $gcd(a, b)$. Conversely, if c is a multiple of $gcd(a, b)$, then one can find integers

α and β such that $a\alpha + b\beta = c$. To do this, work the Euclidean Algorithm backwards to find integers α' and β' such that $a\alpha' + b\beta' = gcd(a, b)$, and then multiply through by the integer $c/gcd(a, b)$.

Fact G3. The integers a and b are relatively prime if and only if there exist integers α and β such that $a\alpha + b\beta = 1$.

You should be able to prove this statement. The main ideas of the proof are contained in the paragraph above. You should also be able to use Fact G3 to prove the following statement.

Fact G4. Let a, b and c be integers. If $a|bc$ and $gcd(a, b) = 1$, then $a|c$.

You should be able to give an example to demonstrate that the statement "If $a|bc$, then $a|b$ or $a|c$" is False. (Thus the hypothesis that $gcd(a, b) = 1$ is important.)

Numbers in Other Bases

The number one hundred and forty-three is usually denoted (in base 10) by 143. What this really stands for is $1 \times 10^2 + 4 \times 10^1 + 3 \times 10^0$. Its an example of our *place-value* system. There is a ones place, a tens place a hundreds place, etc. More generally, if each d_i stands for a digit, then $d_k d_{k-1} \ldots d_1 d_0$ is really a shorthand for $d_k \times 10^k + d_{k-1} \times 10^{k-1} + \ldots + d_1 \times 10^1 + d_0 \times 10^0$.

In base ten we use the digits $0, 1, \ldots, 9$ (from zero up to the base minus one). But there is no real reason to use ten as the base. **Memorize:** If $b > 1$ is an integer and each d_i is an integer between 0 and $b - 1$, then the notation $(d_k d_{k-1} \ldots d_1 d_0)_b$ means $d_k \times b^k + d_{k-1} \times b^{k-1} + \ldots + d_1 \times b^1 + d_0 \times b^0$. If $n = d_k \times b^k + d_{k-1} \times b^{k-1} + \ldots + d_1 \times b^1 + d_0 \times b^0$, then $(d_k d_{k-1} \ldots d_1 d_0)_b$ is called the *base b representation of n*.

If the base is bigger than 10, then we need to use other symbols to represent the digits. For example, in hexadecimal (base 16), the letters A, B, C, D, E, and F stand for 10 through 15, respectively.

Theorem. If $b > 1$, then every integer n has a unique base b representation.

The digits of the base b representation of n, *from right to left*, are the remainders on successive division by b. That is, if $n = bq_0 + r_0, 0 \leq r < b$, then $d_0 = r_0$. Continuing, write $q_0 = bq_1 + r_1, 0 \leq r < b$, and $d_1 = r_1$. Keep repeating the process of dividing the quotient by b and taking the remainder to get the rest of the digits. To see why this works, work backwards from d_k.

Adding and multiplying in base b work just like in base ten. You keep the ones digit and carry the appropriate multiple of the base. Multiplication in base 2 is particularly easy: it just involves shifting and adding.

To convert from base 2 to base 16, work from right to left replacing each group of 4 binary digits by the corresponding hexadecimal digit. (You may need to add a few leading zeros

to make the number of bits a multiple of 4.) Converting from base 16 to base 2 is equally easy: replace each hexadecimal digit by the corresponding 4-digit binary number (you have to use all 4 bits, including leading zeros). Similar rules apply to converting binary to octal (base 8: one octal digit corresponds to three bits), base 4, or any other base which is a power of 2. You should be able to explain in words why these shortcuts work.

Modular Arithmetic

Memorize: If a, b, and m are integers, we say that a *is congruent to* b *modulo* m, and write $a \equiv b (\text{mod } m)$ if $m|a - b$.

You should know how to prove the following facts.

Fact M1. $a \equiv b (\text{mod } m) \quad \Leftrightarrow \quad a = b + km$, for some integer k.

Fact M2. Suppose $a \equiv b (\text{mod } m)$ and $c \equiv d (\text{mod } m.)$ Then,

(i) $a + c \equiv b + d (\text{mod } m)$

(ii) $a - c \equiv b - d (\text{mod } m)$

(iii) $ac \equiv bd (\text{mod } m.)$

The universe of integers (mod m) really only consists of the numbers $0, 1, 2, \ldots, m - 1$; modulo m, any other integer is just one of these with another name. An important implication of Fact M2 is that, when doing calculations (mod m,) you can replace any number by another to which it is congruent, and nothing changes.

You can think of the integers (mod m) as the hours on a circular clock with m hours. Addition corresponds to moving clockwise around the circle an appropriate number of places, subtraction corresponds to moving counter-clockwise. The important part is that the number of times you go around the circle and return to your starting point makes no difference to where you end up. What does matter is the number of places you move when it is no longer possible to make it around the circle any more, and this number is one of $0, 1, 2, \ldots, m - 1$.

By Fact M2 (iii), if $a \equiv b (\text{mod } m)$ and c is an integer, then $ac \equiv bc (\text{mod } m.)$ You should be able to give an example to show that the converse of this statement is False. You should also be able to use Fact G4 (above) to prove the following statement, which says that we can cancel when the number being cancelled is relatively prime to the modulus.

Fact M3. If $ac \equiv bc (\text{mod } m)$ and $gcd(c, m) = 1$ then $a \equiv b (\text{mod } m.)$

In many programming languages there is a function *mod*. If $m \neq 0$ is an integer, then $a (\text{mod } m)$ is the unique number among $0, 1, 2, \ldots, m - 1$ to which a is congruent modulo m. It is the remainder (as in the division algorithm - that's why its unique) when a is divided by m.

It is easy to use congruences to prove the (familiar) rule that an integer is divisible by 3 if and only if the sum of its decimal digits is divisible by 3. The key is to observe that

$10 \equiv 1 (\text{mod } 3)$ and so by Fact M2 (iii) you can change 10 to 1 wherever it occurs. Suppose $n = (d_k d_{k-1} \dots d_1 d_0)_{10}$. Then $n \equiv 0 (\text{mod } 3) \Leftrightarrow d_k \times 10^k + d_{k-1} \times 10^{k-1} + \dots + d_1 \times 10^1 + d_0 \times 10^0 \equiv 0 (\text{mod } 3) \Leftrightarrow d_k \times 1^k + d_{k-1} \times 1^{k-1} + \dots + d_1 \times 1^1 + d_0 \times 1^0 \equiv 0 (\text{mod } 3)$ which is what we wanted.

A similar argument shows that an integer is divisible by 9 if and only if the sum of its decimal digits is divisible by 9, and only a small change is needed to show that $(d_k d_{k-1} \dots d_1 d_0)_{10}$ is divisible by 11 if and only if $d_k - d_{k-1} + d_{k-2} - \dots \pm d_0$ is divisible by 11. It is a good exercise to work through these for yourself.