CSIT 241 Spring 2002

Number Theory Definitions and Facts

Definition: Let a and b be integers. An integer g is said to be a *common divisor* of a and b if g divides both a and b (I.e. if g is a factor of both a and b).

Definition: Let a and b be integers. An integer g is said to be the *greatest common divisor* of a and b, deonted $gcd(b, a)$, if g is the largest common divisor of a and b.

Facts about the greatest common divisor:

Let a and b be integers. Then

1. $gcd(b, a) \geq 1$. Thus, $gcd(b, a)$ is positive.
2. $gcd(b, a) = gcd(a, b) = gcd(-b, a) = gcd(b, -a) = gcd(-b, -a) = gcd(-a, b) = gcd(a, -b) = gcd(-a, -b)$.
3. $gcd(b, 0) = |b|$.

Definition: Let a and b be integers. If $gcd(a, b) = 1$, then a and b are said to be *relatively prime*.

Question: How to find the greatest common divisor?

Answer: Let a and b be integers. Here is how to find $gcd(b, a)$. (Follow the steps in order.)

1. If $b < 0$, let $b = |b|$ and if $a < 0$, let $a = |a|$.
2. If $b < a$, swap b and a; i.e. let temp $= b$, $b = a$, $a =$ temp.
3. Divide b by a and get the quotient and the remainder r.
4. If $r = 0$, then $gcd(b, a) = a$ and stop. If $r \neq 0$, let $b = a$ and $a = r$ and go to step 3.

Note: The above algorithm is called the Euclidean algorithm.

Note: To find $gcd(b, a)$, if both a and b are negative or one of them is negative, remove the negative sign.

Here is a c++ function that computs $gcd(b, a)$ for any integers a and b.

```
int gcd(int b, int a)
{
    int r;
    if (a < 0) a = abs(a);
    if (b < 0) b = abs(b);
    if (b < a)
    {
        int temp = b;
        b = a;
        a = temp;
    }
    while (a != 0)
    {
        r = b % a;
        b = a;
        a = r;
    }
    return b;
}
```

Definition: Let a and b be intgers. An integer l is said to be a *common multiple* of a and b if l is a multiple of both a and b; i.e. both a and b are factors of l.

Definition: Let a and b be intgers. l is said to be *the least common multiple* of a and b, denoted $lcm(a, b)$, if l is the smallest *positive* common multiple of a and b.

Question: How to find the least common multiple?

Answer: To find $lcm(b, a)$, where a and b are nonzero integers, find $gcd(b, a)$ first. Then $lcm(b, a)$ is given by $lcm(b, a) = \frac{|ba|}{gcd(b,a)}$.

Facts about the least common multiple:

Let a and b be nonzero integers. Then

$lcm(b, a) = lcm(a, b) = lcm(-b, a) = lcm(b, -a) = lcm(-b, -a) = lcm(-a, b) = lcm(a, -b) = lcm(-a, -b)$.

Extended Euclidean Algorithm

Let a and b be integers. To find $gcd(b, a)$ and write it as a linear combination of b and a; i.e. to write $gcd(b, a) = \beta b + \alpha a$. Without loss of generality, assume $b > a > 0$. Then form the following matrix:

$b \quad 1 \quad 0$

$a \quad 0 \quad 1$

Each row after the first two is of the form $x - qy$, where x and y are the two rows proceeding it (in order) and q is the quptient when the first number in x is divided by the first number in y. Keep forming new rows and stop when you get a row in which the first number is zero. Then $gcd(b, a)$ is the first number of the proceeding row and β and α are the second and third (respectively) numbers in that row.

Question: If a or b are negative ot at least one of them is negative, then how to find $gcd(b, a)$ and write it as a linear combination of them?

Answer: First find $gcd(|b|, |a|)$ and write it as a linear combination of $|a|$ and $|b|$. The reamining part of the answer will be explained in class.