MATH 289
PROBLEM SET 4: NUMBER THEORY

1. The greatest common divisor

If d and n are integers, then we say that d divides n if and only if there exists an integer q such that $n = qd$. Notice that if d divides n and m, then d also divides $n + m$ and $n - m$ and $an + bm$ for all integers a, b.

Theorem 1. *If n and m are integers and $m \neq 0$, then there exists an integer q such that*

$$n = qm + r$$

where $0 \leq r < |m|$.

Proof. First reduce to the case that $n \geq 0$. Then use induction on n. (Exercise.) □

A useful variation is the following result.

Theorem 2. *If n and m are integers and $m \neq 0$, then there exists an integer q such that*

$$n = qm + r$$

where $-|m|/2 \leq r < |m|/2$.

Suppose that n and m are integers, not both equal to 0. The greatest common divisor of n and m is the largest *positive* integer d such that d divides both n and m. We denote the greatest common divisor of n and m by $\gcd(n, m)$. We will also use the convention that $\gcd(0, 0) = 0$. The following observation will be useful.

Lemma 3. *If $n, m, q \in \mathbb{Z}$, then We have $\gcd(n, m) = \gcd(m, n - qm)$.*

Proof. The case $n = m = 0$ is clear. Assume that at least one of n and m is nonzero. Now $\gcd(n, m)$ divides n, m and $n - qm$, hence

$$\gcd(n, m) \leq \gcd(m, n - qm).$$

On the other hand, $\gcd(m, n - qm)$ divides m, $n - qm$ and $n = (n - qm) + qm$. so

$$\gcd(m, n - qm) \leq \gcd(n, m).$$

□

Example 4. Suppose we have two large integers, say 9081 and 3270. How do we find their greatest common divisor? We do division with remainder:

$$9081 = 3 \cdot 3270 - 729.. \tag{1}$$

Now $\gcd(9081, 3270) = \gcd(3270, 729)$. We have simplified our problem! Now we can play this game again:

$$3270 = 4 \cdot 729 + 354. \tag{2}$$

so $\gcd(3270, 729) = \gcd(729, 354)$.

$$729 = 2 \cdot 354 + 21 \tag{3}$$

so $\gcd(729, 354) = \gcd(354, 21)$.

$$354 = 17 \cdot 21 - 3 \tag{4}$$

so $\gcd(354, 21) = \gcd(21, 3) = 3$ because $21 = 7 \cdot 3$. We have found that $\gcd(9081, 3270) = 3$. This method of computing the gcd is called Euclid's algorithm.

Algorithm 5 (Euclid's Algorithm)**.** Suppose that $r_0, r_1 \in \mathbb{Z}$ are nonzero integers. Define $q_1, q_2, \cdots \in \mathbb{Z}$ and $r_2, r_3, \cdots \in \mathbb{Z}$ inductively as follows. If r_{i-1} and r_i are already defined, then we define q_i and r_{i+1} by

$$r_{i-1} = q_i r_i + r_{i+1}$$

where $0 \leq r_{i+1} < |r_i|$ as in Theorem 1 (or $-|r_i|/2 \leq r_{i+1} < |r_i|/2$ as in Theorem 2). (Note r_{i+1} and q_i are well defined as long as $r_i \neq 0$).

Since $|r_1| > |r_2| > \cdots$ we have that $r_{k+1} = 0$ for some positive integer k. Suppose that $r_{k+1} = 0$ and that $r_i \neq 0$ for $i \leq k$. Then $\gcd(r_0, r_1) = r_k$.

If one uses Theorem 2 then it is clear that Euclid's algorithm is very fast. The number of divisions with remainder one has to do is roughly $\log_2 |r_1|$. (A similar bound also holds if one uses Theorem 1 though).

Proof. It is not hard to show that Euclid's algorithm works. Note that $\gcd(r_{i-1}, r_i) = \gcd(r_i, r_{i+1})$ for all i. By induction on i one shows that $\gcd(r_0, r_1) = \gcd(r_i, r_{i+1})$ for all i. In particular,

$$\gcd(r_0, r_1) = \gcd(r_k, r_{k+1}) = \gcd(r_k, 0) = r_k.$$

☺

Example 6. Euclid's algorithm can be used to find integers x and y such that $\gcd(n, m) = xn + ym$. It works as follows. First use Euclid's algorithm to compute $\gcd(n, m)$ and then work back. For example, we already saw that $\gcd(9081, 3270) = 3$. We would like to find x and y such that

$$3 = 9081x + 3270y.$$

Now we work back in the computation of $\gcd(9081, 3270)$. From (4) follows that

$$3 = (-1) \cdot 354 + 17 \cdot 21.$$

From (3) follows that

$$3 = (-1) \cdot 354 + 17 \cdot (729 - 2 \cdot 354) = 17 \cdot 729 + (-1 - 17 \cdot 2) \cdot 354 = 17 \cdot 729 - 35 \cdot 354.$$

From (2) follows that

$$3 = 17 \cdot 729 - 35 \cdot (3270 - 4 \cdot 729) =$$
$$= -35 \cdot 3270 + (17 + 35 \cdot 4) \cdot 729 = -35 \cdot 3270 + 157 \cdot 729.$$

and finally, from (1) follows that

$$3 = -35 \cdot 3270 + 157 \cdot (-9081 + 3 \cdot 3270) =$$
$$= -157 \cdot 9081 + (-35 + 3 \cdot 157) \cdot 3270 = -157 \cdot 9081 + 436 \cdot 3270.$$

This method is sometimes called the *extended Euclid's algorithm.*

Algorithm 7. (Extended Euclid's Algorithm) Let $r_0, r_1, \ldots, r_k, r_{k+1} = 0$ and $q_0, q_1, \ldots, q_k$ as in Algorithm 5.

Define $x_k = 0$ and $x_{k+1} = 1$. For $i \geq 1$, define x_{k-i} by induction by

$$x_{k-i-1} = x_{k-i+1} - q_{k-i}x_{k-i}.$$

Then we have that

$$\gcd(r_0, r_1) = x_{i+1}r_i + x_i r_{i+1}$$

for $i = 0, 1, \ldots, k$. In particular,

$$\gcd(r_0, r_1) = x_1 r_0 + x_0 r_1.$$

Proof. Let $i = k - j$. We prove by induction on j that

$$\gcd(r_0, r_1) = x_{k-j+1}r_{k-j} + x_{k-j}r_{k-j+1}.$$

For $j = 0$ we have to prove that

$$\gcd(r_0, r_1) = 1 \cdot r_k + 0 \cdot r_{k+1} = r_k$$

but this follows from Algorithm 5.

Suppose that

$$\gcd(r_0, r_1) = x_{k-j+1}r_{k-j} + x_{k-j}r_{k-j+1}.$$

If we substitute, $r_{k-j+1} = r_{k-j-1} - q_{k-j}r_{k-j}$ we obtain

$$\gcd(r_0, r_1) = x_{k-j+1}r_{k-j} + x_{k-j}(r_{k-j-1} - q_{k-j}r_{k-j}) =$$
$$= x_{k-j}r_{k-j-1} + (x_{k-j+1} - q_{k-j}x_{k-j})r_{k-j} = x_{k-j}r_{k-j-1} + x_{k-j-1}r_{k-j}.$$

☺

Theorem 8. *Suppose that n and m are integers. There exist integers x and y such that*

$$\gcd(n, m) = xn + ym.$$

Proof. This follows from the extended Euclid's Algorithm (Algorithm 7). ☺

If n and m are integers with $\gcd(n, m)$ then we say that m and n are *relatively prime.*

Corollary 9. *If a, n, m are integers and a divides both n and m then a also divides $\gcd(n, m)$.*

Proof. This follows immediately from the previous Theorem 8. □

Example 10 (Putnam 2000)**.** Prove that the expression

$$\frac{\gcd(m, n)}{n}\binom{n}{m}$$

is an integer.

Given our previous discussion, it seems natural to write

$$\gcd(m,n) = xm + yn$$

where x, y are integers. The solution then follows quickly.

Proof. We can write

$$\gcd(m,n) = xm + yn$$

where $x, y \in \mathbb{Z}$. Then

$$\frac{\gcd(m,n)}{n}\binom{n}{m} = x\binom{n}{m} + y\frac{m}{n}\binom{n}{m}.$$

Now

$$\frac{m}{n}\binom{n}{m} = \frac{m}{n}\frac{n!}{m!(n-m)!} = \frac{(n-1)!}{(m-1)!(n-m)!} = \binom{n-1}{m}$$

is an integer. It follows that

$$\frac{\gcd(m,n)}{n}\binom{n}{m}$$

is an integer. ☺

Lemma 11. *Suppose that n, m, r are integers such that $\gcd(m,n) = 1$. If m divides nr then m divides r.*

Proof. We can write $1 = xm + yn$ for certain $x, y \in \mathbb{Z}$. Clearly m divides xmr and ynr, so m divides

$$r = r \cdot 1 = r \cdot (xm + yn) = xmr + ynr.$$

□

If n and m are nonzero integers then the least common multiple $\operatorname{lcm}(m,n)$ of n and m is defined as the smallest positive integer that is divisible by both m and n. Moreover we define $\operatorname{lcm}(m,0) = 0$ for all integers m.

Lemma 12. *If n and m are positive integers and a is an integer divisible by both n and m, then a is divible by $\operatorname{lcm}(m,n)$.*

Proof. We can write $a = q\operatorname{lcm}(m,n) + r$ with $0 \leq r < \operatorname{lcm}(m,n)$. NOw r is also divisible by m and n. We must have that $r = 0$ otherwise we get a contradiction with the definition of $\operatorname{lcm}(m,n)$. This proves that a is divisible by $\operatorname{lcm}(m,n)$. □

Lemma 13. *If n and m are positive integers then*

$$\gcd(m,n)\operatorname{lcm}(m,n) = mn$$

Proof. The positive integer $mn/\gcd(m,n)$ is divisible by m and n, so

$$\frac{mn}{\gcd(m,n)} \geq \operatorname{lcm}(m,n).$$

The positive integer $mn/\operatorname{lcm}(m,n)$ divides both m and n.So we have

$$\frac{mn}{\operatorname{lcm}(m,n)} \leq \gcd(m,n).$$

□

Example 14. In the strange country Oz, the only official coins are the 7-cents coin and the 13-cents coin. What is the largest amount that cannot be paid with these coins if a shop has no change at all?

We can first make a list of amounts that we can make:

$$7, 13, 14, 20, 21, 26, 27, 28, 33, 34, 35, 39, 40, 41, 42, 46, 48, 48, 49, 52, 53, 54, 55, 56,$$

$$59, 60, 61, 62, 63, 65, 66, 67, 68, 69, 70, 72, 73, 74, 75, 76, 77, 78, 79, \ldots$$

The largest amount that cannot be made seems to be 71. It is easy to check that 71 is not a nonnegative combination of 7 and 13.

Let us try to understand why all the amounts of ≥ 72 can be made by using the two types of coins. Suppose that $m \geq 72$. We would like to find nonnegative integers x and y such that

$$m = 13x + 7y$$

If x and y are not necessarily nonnegative then this is certainly possible. We can write

$$1 = 13 \cdot (-1) + 7 \cdot 2$$

and

$$m = 13 \cdot (-m) + 7 \cdot 2m.$$

Using this solution we find many other solutions. If k is an integer then

$$m = 13 \cdot (-m + 7k) + 7 \cdot (2m - 13k).$$

For a suitable k, we might have that both $-m+7k$ and $2m-13k$ are nonnegative. Consider the smallest k for which $-m + 7k$ is nonnegative. Then we have $0 \leq -m + 7k < 7$. Now

$$7 \cdot (2m - 13k) \geq m - 13 \cdot (-m + 7k) \geq 72 - 13 \cdot 6 = -6.$$

It follows that $2m - 13k > -1$, so $2m - 13k$ is nonnegative.

Now we would like to prove that if

$$71 = 13x + 7y \tag{5}$$

with $x, y \in \mathbb{Z}$, then at least one of the integers x, y is negative. We already saw one solution, namely

$$71 = 13 \cdot (-71) + 7 \cdot (142). \tag{6}$$

Combining (5) and (6) yields:

$$13 \cdot (x + 71) = 7 \cdot (142 - y).$$

Since $\gcd(13, 7) = 1$, we have that 7 divides $x + 71$. Say $x + 71 = 7k$. Then we alsy have that $142 - y = 13k$. From $x + 71 = 7k$ and $x \geq 0$ follows that $k \geq 11$. But then $y = 142 - 13k \leq -1$.

2. Prime Numbers

Recall that a prime number is a positive integer with exactly 2 positive divisors, namely 1 and itself.

Lemma 15. *If p is a prime number dividing mn where m and n are integers, then p divides m or p divides n.*

Proof. If p divides m then were are done. Otherwise $\gcd(p, m) = 1$, so p divides n by Lemma 11. □

Theorem 16. *(Euclid) Every positive integer can uniquely be written as a product of prime numbers.*

Proof. We already have seen in problem set 1 that every positive integer is a product of prime numbers. We still have to prove the uniqueness. Suppose that $p_1 < p_2 < \cdots < p_k$ are distinct prime numbers such that

$$p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k} = p_1^{b_1} p_2^{b_2} \cdots p_k^{a_k}.$$

Suppose that $a_1 > b_1$. Then

$$p_1^{a_1 - b_1} p_2^{a_2} \cdots p_k^{a_k} = p_2^{b_2} \cdots p_k^{a_k}$$

and p_1 divides $p_2^{b_2} \cdots p_k^{a_k}$. This implies that p_1 divides p_i for some $i \geq 2$. This is impossible because the only divisors of p_i are 1 and p_i itself. Constradiction. Therefore $a_1 \leq b_1$. Similarly we see that $a_1 \geq b_1$ and therefore $a_1 = b_1$. Similarly we can prove that $a_i = b_i$ for $i = 2, 3, \ldots k$. □

Many properties can be expressed in terms of the prime factorization. Suppose that

$$A = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$$

and

$$B = p_1^{b_1} p_2^{b_2} \cdots p_k^{b_k}$$

are positive integers with their factorizations into prime numbers. Then A divides B if and only if $a_i \leq b_i$ for all $i = 1, 2, \ldots, k$. We also have that

$$\gcd(A, B) = p_1^{c_1} p_2^{c_2} \cdots p_k^{c_k}$$

where $c_i = \min(a_i, b_i)$ for all i.

Theorem 17. *(Euclid) There are infinitely many prime numbers.*

Proof. Suppose that there are finitely many distinct prime numbers, say $p_1, p_2, \ldots, p_k$. Let $N = p_1 p_2 \cdots p_k + 1$. Now N is a product of prime numbers. In particular there exists a prime numper q such that q divides N. Now $q = p_i$ for some i with $1 \leq i \leq k$. Since p_i divides N, we have that p_i divides

$$N - p_1 p_2 \cdots p_k = 1$$

which leads to a contradiction. □

Example 18. The number $\sqrt{2}$ is irrational.

Proof. Suppose taht $\sqrt{2}$ is rational, say $\sqrt{2} = p/q$ where p, q are positive integers. Squaring gives $p^2 = 2q^2$. The prime number 2 appears an even number of time in the prime factorization of p^2. On the other hand, 2 appears an odd number of times in the prime factorization of $2q^2$. Wet get a contradiction, so $\sqrt{2}$ has to be irrational. □

The distribution of prime numbers is quite mysterious. One of the most famous/notorious open problems in mathematics is the Riemann Hypothesis. This conjecture is closely related to the distribution of prime numbers. The following result is well-known but not so elementary:

Theorem 19 (Dirichlet)**.** *Suppose that a and b are positive integers that are relatively prime. Then there are infinitely prime numbers of the form $a + nb$ where n is a positive integer.*

3. Exercises

Exercise 1. ** Let $F_0, F_1, F_2, \ldots$ be the Fibonacci numbers: $F_0 = F_1 = 1$ and $F_{n+1} = F_n + F_{n-1}$ for all $n \geq 1$. Prove that the greatest common divisor of two consecutive Fibonnaci numbers is always equal to 1.

Exercise 2. *** Define $T_0, T_1, T_2, \ldots$ by $T_1 = 2$ and $T_{n+1} = T_n^2 - T_n + 1$ for $n \geq 0$. Prove that $\gcd(T_i, T_j) = 1$ for all $i \neq j$.

Exercise 3. **** Let $m \geq 2$ be an integer and suppose that a and b are positive integers. Prove that

$$\gcd(m^a - 1, m^b - 1) = m^{\gcd(a,b)} - 1.$$

Exercise 4. ** We have two drinking glasses. One glass can contain exactly 21oz. The other glass can contain exactly 13oz. Is it possible to measure exactly 1oz. of water using the two glasses?

Exercise 5. ** Suppose that

$$A = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$$

is an integer, $p_1 < p_2 < \cdots < p_k$ are distinct primes and $a_1, \ldots, a_k$ are nonnegative integers. Give a formula for the number of divisors of A.

Exercise 6. *** We start with a deck of 52 cards. We put all the cards in one row, face down. In the first round we turn all the cards around. In the second round we turn every second card around. In the third round we turn every third card around. We keep doing this until we complete round 52. Which cards will be faced up in the end?

Exercise 7. *** Suppose that $P(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0$ is a nonconstant polynomial with integer coefficients. Prove that there exists a positive integer m such that $|P(m)|$ is not a prime number.

Exercise 8. ** Show that there are infinitely many prime numbers of the form $4k - 1$ where k is a positive integer (without using Dirichlet's Theorem).

Exercise 9. * Find all prime numbers p for which $p + 2$ and $p + 4$ are also prime numbers.

Exercise 10. * Use Euclid's Algorithm to find $\gcd(1029, 791)$.

Exercise 11. **** Suppose that p, q, r are positive integers which $\gcd(p, q) = \gcd(p, r) = \gcd(q, r) = 1$. Show that if $N \geq 3pqr$, then any $N \times N$ floor can be tiled with tiles of sizes $p \times p$, $q \times q$ and $r \times r$.

Exercise 12. ** Suppose that m and n are positive integers with $\gcd(m, n) = 1$. Show that $mn - m - n$ is the largest integer that is not of the form $mx + ny$ with $x, y \geq 0$.

Exercise 13. ** Show that if $2^n - 1$ is a prime number, then n is a prime number.

Exercise 14. ** Show that if $2^n + 1$ is a prime number, then $n = 0$ or n is a power of 2.