18.781
PROBLEM SET 1

JOHN WANG

1. Problem 1

Problem 1.1. *Let $a > 0$ and b be integers. Show that there is an integer k such that $b + ka > 0$.*

Solution Let us examine the set $S = \{b + ka | b + ka > 0; a, b \in \mathbb{Z}; a > 0\}$. This set is nonempty because if $b \geq 0$, then we can simply take $k = 1$ and $b + ka > 0$. Otherwise, if $b < 0$, then there exists some k such that $b + ka > 0$. This is because $b = qa + r < (q + 1)a$ for some $q \in \mathbb{Z}$ and $0 \leq r < a$. Thus, simply take $k = q + 1$ and we see that $b + ka > 0$. Thus, the set S is nonempty and one can use the well ordering principle to select the smallest element from the set. This shows the existence of an integer k for which $b + ka > 0$. $\square$

2. Problem 2

Problem 2.1. *Let a and b be positive integers whose gcd is 1. Find the largest positive integer $n(a, b)$ which is not a non-negative integer linear combination of a and b.*

Solution Let us examine the sets $S = \{ax + by | 0 \leq x < b; y \geq 0\}$ and $U = \{ax + by | ax + by > 0; 0 \leq x < b; y < 0\}$. One can see that the set S contains all the integers which can be expressed as a non-negative linear combination of a and b. Also, the set U spans the positive integers which can be expressed as negative linear combinations of a and b. It is clear that the largest positive integer n which cannot be expressed as a non-negative integer linear combination of a and b is the maximum element in U.

Therefore, we must first show that U is nonempty and invoke the well ordering principle to select the maximum. First, we can assume without loss of generality that $a > b$ because $(a, b) = 1$. Then, we can simply choose $y = -1$ and we see that $ax - b \in U$. Since $0 \leq x < b$, we see that $x \geq 1$ which means that $ax - b > 0$ and is therefore in U. Because the set is nonempty, we can select its maximum.

In fact, the maximum is when $x = b - 1$ and $y = -1$ because both $x, y \in \mathbb{Z}$. Therefore, we see that the maximum positive integer which cannot be represented as a non-negative linear combination of a and b is:

$$\begin{aligned} a(b-1) + b(-1) &= a(b-1) - b \\ &= ab - a - b \end{aligned} \tag{2.1}$$

Therefore, we have found that $n = ab - a - b$. $\square$

3. Problem 3

Problem 3.1. *Let $a > 1$ be a positive integer and m, n be natural numbers. Show that $a^m - 1 | a^n - 1$ if and only if $m | n$.*

Solution First we shall assume $m|n$ and show that $a^m - 1 | a^n - 1$. Since $m|n$, we see that $n = dm$ for some $d \in \mathbb{Z}$. Therefore, we have $a^n - 1 = a^{md} - 1$. Moreover, we can factor $a^{md} - 1$ into the following:

$$a^{md} - 1 = a^{md} - 1 + (a^{m(d-1)} - a^{m(d-1)} + \ldots + a^m - a^m) \tag{3.1}$$

$$= (a^m - 1)(a^{m(d-1)} + a^{m(d-2)} + \ldots + a^m + 1) \tag{3.2}$$

But this implies that $a^m - 1$ is a factor of $a^{md} - 1$ and therefore that $a^m - 1 | a^{md} - 1 = a^n - 1$.

Now we shall assume $a^m - 1 | a^n - 1$ and prove that $m|n$. First, we note that if $a^m - 1 | a^n - 1$, then $a^m - 1 | a^n - 1 - (a^m - 1)$. Therefore, we see that:

$$a^m - 1 \quad | \quad a^n - a^m \tag{3.3}$$

$$a^m - 1 \quad | \quad a^m(a^{n-m} - 1) \tag{3.4}$$

Since we assumed that $a > 1$, we see that $(a^m - 1, a^m) = 1$. Therefore, we know that $a^m - 1 \nmid a^m$ so we can write:

$$a^m - 1 \quad | \quad a^{n-m} - 1 \tag{3.5}$$
$$a^m - 1 \quad | \quad a^{n-m} - 1 - (a^m - 1) \tag{3.6}$$
$$a^m - 1 \quad | \quad a^{n-m} - a^m \tag{3.7}$$
$$a^m - 1 \quad | \quad a^m(a^{n-2m} - 1) \tag{3.8}$$

By the same argument as above that $(a^m - 1, a^m) = 1$, we see that $a^m - 1 | a^{n-2m} - 1$. If we iterative this argument, we see that this will eventually terminate because the exponent is strictly decreasing. Therefore, there will be some $d \in \mathrm{N}$ at which we terminate and for which $a^m - 1 | a^{n-dm} - 1$. But we see that this terminates exactly when $n - dm = m$. Therefore, we see that $n = m(d + 1)$ for some $d > 0$. Thus, we see that $m|n$. $\square$

Problem 3.2. *Show that* $(a^m - 1, a^n - 1) = a^{(m,n)} - 1$.

Solution We will use the same proof structure as above. We know that $(a, b) = (a, b - a)$ if $b > a$. We assume WLOG that $n > m$ so that $(a^m - 1, a^n - 1) = (a^m - 1, a^n - a^m)$. This means we have:

$$(a^m - 1, a^n - 1) \quad = \quad (a^m - 1, a^m(a^{n-m} - 1)) \tag{3.9}$$
$$= \quad (a^m - 1, a^{n-m} - 1) \tag{3.10}$$

By the same argument as before, namely that since $a > 1$, then $(a^m - 1, a^m) = 1$ so that $a^m - 1 \nmid a^m$. Iterating this process is simply the Euclidean algorithm on the exponents, which means that we will eventually reach $a^{(m,n)} - 1$. $\square$

4. Problem 4

Problem 4.1. *Use the Euclidean algorithm to find an integer solution* (x_0, y_0) *to* $89x + 43y = 1$. *Then use your solution to describe all possible integer solutions systematically.*

Solution The Euclidean algorithm will be used in the table below:

Quotient	Divisor	Vector	
	89	1	0
2	43	0	1
14	3	1	-2
	1	-14	29

Table 1. Euclidean Algorithm for $89x + 43y = 1$

Thus, we can use $x_0 = -14$ and $y_0 = 29$ to obtain $(89)(-14) + (43)(29) = 1$. Moreover, every integer solution can be described by subtracting x_0 and y_0 from 89 and 43 respectively. This shows that $x = 43a + 29$ and $y = -89a - 60$ will describe all integer solutions to $89x + 43y = 1$. This is because when we substitute x and y into the equation, we obtain $89(43a + 29) + 43(-89a - 60) = (89)(29) - (43)(60) = 1$ which is what we wanted. $\square$

5. Problem 5

Problem 5.1. *Let* $1 < a < b$ *be integers. Show that the number of divisions steps involved in the Euclidean algorithm to compute the gcd of* a *and* b *is at most a universal constant times* $\log(a)$.

Solution Let us start the algorithm with $a = a_0$ and $b = b_0$. The next step of the algorithm will use the integers $a_1 < b_1$ and so on until termination at the $n + 1$st step. We shall show that $a_{i+1} \leq pa_i$ for some constant $p < 1$ for all $i \in \{1, \dots, n\}$. To show this, we choose $p = \frac{a-1}{a}$. On the first step, since $a = a_0$, we see that $a_1 \leq pa_0 = (a - 1)$. This is because a is strictly decreasing in the Euclidean algorithm because $r < a$. Moreover, $a_{i+1} \leq pa_i$ for all $i \in \{1, \dots, n\}$ because a_i is strictly decreasing. This means the largest value of a_i for any i is a, and the smallest decrement occurs from a to $a - 1$. Since this can only possibly occur on the first step, and since $a_{i+1}/a_i \leq (a - 1)/a = p$ for all greater i, we see that $a_{i+1} \leq pa_i$.

We know the algorithm terminates, so let us say that the value of the smaller number in the second to last step is d. Since we have shown that $a_{i+1} \leq pa_i$, we know that $d \leq p^n a$. Taking logarithms of both sides, and noting that $p < 1$, we see that $\log_p(d/a) \geq n$. Since $d < a$ by the strictly decreasing nature of the algorithm, we see that $n \leq \log_p(d/a) < \log_p(a) = \log(a)/\log(p) = c\log(a)$. Therefore, we have found that $n < c\log(a)$. $\square$

6. Problem 6

Problem 6.1. *Using the math software gp/PARI, tabulate the number of primes less than x for $x = 10000, 20000, \ldots, 100000$. Also tabulate the number of primes less than x and of the form $4k+1$ and the number of the form $4k+3$ and also $x/\log(x)$.*

Solution The gp/PARI code for this exercise is given below:

```
for(i=1, 10,
    p = 0;
    p4k3 = 0;
    p4k1 = 0;
    forprime(x=1, i*10000,
        p ++;
        if((x%4) == 3, p4k3 ++, p4k1 ++);
    );
    xlogx = round(i*10000/log(i*10000));
    print("x=", i*10000);
    print("Primes: ", p);
    print("4k+1 Primes: ", p4k1);
    print("4k+3 Primes: ", p4k3);
    print("x/log(x): ", xlogx);
    print(" ");
)
```

The output shows that the number of primes of the form $4k+1$ and $4k+3$ seem to generally be very close together. For $x = 10000$, the $4k+1$ primes have a count of 610 while the $4k+3$ primes have 619. This trend continues for all x that were tested. Moreover, the total number of primes is equal to the sum of the primes of the form $4k+1$ and the form $4k+3$. Moreover, $x/\log(x)$ comes close to the total number of primes but gets further off as x grows larger. □

7. Problem 7

8. Problem 8

Lemma 8.1. *If N is of the form $4k+3$ for $k \geq 1$, then one of its prime factors must also have the form $4k+3$.*

Proof. We shall proceed by induction. For $k = 1$, we find that $4k+1 = 7$ is a prime, so clearly it has a prime factor of the form $4k+3$. Using this as a base case, let us assume that we have shown the assumption true for $k = 1, \ldots, n-1$. We must now show that $N = 4n+3$ has a prime factor of the form $4k+3$.

First, if N is prime, then the proof is complete. Otherwise, we can factor N into components. Since $N = 4n+3$, we can have any of the following factorizations:

$$N = (4a+1)(4b+1) = 4(4ab+1a+1b)+1 \tag{8.2}$$

$$N = (4a+1)(4b+3) = 4(4ab+3a+1b)+3 \tag{8.3}$$

$$N = (4a+3)(4b+3) = 4(4ab+3a+3b+2)+1 \tag{8.4}$$

This follows firstly because $N = 4n+3$ is odd, so its two factors must also be odd. Moreover, the only odd numbers possible are of the form $4k+1$ or $4k+3$. Now, we see that cases 1 and 3 are impossible because they are both of the form $4k+1$. Thus, the second case is the only possibility for factoring N. In this case, we see that $q = (4b+3)$ is a factor of N. By the inductive hypothesis, $q < N$ so that q has a prime factor of the form $4k+3$. Thus, we have shown that N has a prime factor of the form $4k+3$. □

Problem 8.1. *Show that there are infinitely many primes of the form $4k+3$.*

Solution Suppose there are a finite number of primes of the form $4k+3$, denoted by $p_1, \ldots, p_n$. Then we can construct a number $d = 4(p_1 \ldots p_n) - 1 = 4(p_1 \ldots p_n - 1) + 3$ which cannot be a prime because it is larger than any p_i and is of the form $4k+3$. From our lemma, we see that d must have a prime factor of the form $4k+3$. However, this prime factor cannot be one of $p_1, \ldots, p_n$ because $d = qp_i - 1$ for some $q \in \mathrm{Z}$. Therefore, p_i does not divide evenly into d for all $i \in \{1, \ldots, n\}$. Thus, it must be some other prime of the form $4k+3$, which is a contradiction. □