HOMEWORK 3, DUE OCT 4

You must prove your answer to every question.

Problem 1. (10) We have seen in class that if $\gcd(a, b) = 1$ then there is a pair (r_0, s_0) of integers with the property $ar_0 + bs_0 = 1$. Show that any other pair (r, s) of integers satisfies $ar + bs = 1$ if and only if there is an integer t such that $r = r_0 + bt$, $s = s_0 - at$.

Solution. Assume $r = r_0 + bt$, $r = s_0 - at$. Then we have

$$ar + bs = ar_0 + abt + bs_0 - bat = 1.$$

Assume now $ar + bs = 1$. Then we have

$$\begin{aligned} 0 &= (ar + bs) - (ar_0 + bs_0), \\ 0 &= a(r - r_0) + b(s - s_0), \\ a(r - r_0) &= -b(s - s_0). \end{aligned}$$

Since a and b are relatively prime, the last equality implies $b|(r - r_0)$, hence we can write $r - r_0 = bt$ for some integer t, so we have $abt = -b(s - s_0)$, hence $s - s_0 = -at$.

Problem 2 (Exercise 1.8 of Shoup)**.** (10) Let a, b, c be positive integers, with $\gcd(a, b) = 1$ and $c \geqslant ab$. Show that there exist *non-negative* integers s, t giving $c = as + bt$. [Hint: relying on the result of the previous exercise, use the smallest nonnegative s with $c = as + bt$.]

Solution. Using results of the previous exercise, if s_0 is an integer that occurs in some solution of $ax + bt = 1$ then all integers of the form $s_0 + ib$, $i \in \mathbb{Z}$ have this property. Let s_1 be the smallest positive integer in this set, then $s_1 < b$. Then we have $c = as_1 + bt_1 < ab + bt_1$, hence $c - ab < bt_1$, showing $t_1 > 0$.

Problem 3 (Generalization of Exercise 1.10 of Shoup)**.** (10) Show that if a, b, n are integers and a, b both divide n then $\mathrm{lcm}(a, b)$ divides n.

Solution. For a prime number p, we denoted by $\nu_p(x)$ the exponent of p in the prime decomposition of x. If both a, b divide n then $\nu_p(a), \nu_p(b) \leqslant \nu_p(n)$. But then $\max(\nu_p(a), \nu_p(b)) \leqslant \nu_p(n)$. But $\max(\nu_p(a), \nu_p(b)) = \nu_{\mathrm{lcm}(a,b)}(p)$. Since this is true for each p, each prime power in the decomposition of $\mathrm{lcm}(a, b)$ divides n and therefore $\mathrm{lcm}(a, b)|n$.

Problem 4 (Exercise 1.12 of Shoup)**.** (10) Let p be a prime and k an integer $0 < k < p$. Show that the binomial coefficient $\binom{p}{k}$ (which is an integer, of course) is divisible by p.

Solution. A formula you learned for the computation of the binomial coefficient is

$$\binom{p}{k} = \frac{p!}{k!(p - k)!}.$$

On the right-hand side, the numerator is divisible by p but neither factor of the denominator is, since they are products of numbers smaller than p. Therefore the fraction (which is known to be integer) is divisible by p.

Problem 5 (Exercise 1.15 of Shoup)**.** (10) Show that if an integer cannot be expressed as a square of an integer, then it cannot be expressed as a square of any rational number.

Solution. Suppose that the integer x cannot be expressed as a square of an integer. We suppose that $x = (a/b)^2$ for some a, b and get a contradiction. Without loss of generality we can assume that a/b is in its lowest terms, that is $\gcd(a, b) = 1$. Writing $nb^2 = a^2$ we see that we must have $b = 1$ since the right-hand side contains no prime divisors of b. But $n = a^2$ was excluded by our assumption.

Problem 6 (Exercise 1.21 of Shoup)**.** (10) Show that for any $a_1, \ldots, a_k \in \mathbb{Z}$, if $d := \gcd(a_1, \ldots, a_k)$, then $d\mathbb{Z} = a_1\mathbb{Z} + \cdots + a_k\mathbb{Z}$; in particular, there exist integers $s_1, \ldots, s_k$ such that $d = a_1s_1 + \cdots + a_ks_k$.

Solution. The statement $d\mathbb{Z} \supseteq a_1\mathbb{Z} + \cdots + a_k\mathbb{Z}$ comes from the definition: since d is a common divisor of $a_1, \ldots, a_k$, $d\mathbb{Z}$ contains all the sets $a_i\mathbb{Z}$ and therefore also their sum.

We will prove the existence of the expression $d = a_1s_1 + \cdots + a_ks_k$ by mathematical induction on k. We have proved it in class for $k = 2$, so assume that $k > 2$. Let $d_2 = \gcd(a_2, \ldots, a_k)$. First note $\gcd(a_1, \ldots, a_k) = \gcd(a_1, d_2)$. Indeed, this follows from the equation

$$\max(e_1, \ldots, e_k) = \max(e_1, \max(e_2, \ldots, e_k))$$

applied to the exponents $e_i = \nu_p(a_i)$ of the primes.

By the inductive assumption we know $d_2 = t_2a_2 + \cdots + t_ka_k$ for some integer t_i. Also by the case $k = 2$ we know $d = u_1a_1 + u_2d_2$ for some integer u_i. Combining these we get

$$d = u_1a_1 + (u_2t_2)a_2 + \cdots + (u_kt_k)a_k.$$