HOMEWORK ASSIGNMENT #2 SOLUTIONS

(1) Let $a_1, \ldots, a_n$ be nonzero integers. For what values of d does the equation $a_1x_1 + \ldots + a_nx_n = d$ have integer solutions $x_1, \ldots, x_n$?

Solution. The answer is whenever d is a multiple of $\gcd(a_1, \ldots, a_n)$. We will prove this by induction on the number of variables $x_1, \ldots, x_n$, with $n = 2$ being the base case.

The $n = 2$ base case is just a restatement of the main theorem (Theorem 1.13) about solving linear equations in two variables in integers. We've already proved this, so let's consider the case with $n + 1$ variables , assuming that the case with n variables is true.

Consider the expression $a_1x_1 + \ldots + a_nx_n + a_{n+1}x_{n+1}$. The set of d such that $a_1x_1 + \ldots + a_nx_n + a_{n+1}x_{n+1} = d$ has a solution $x_1, \ldots, x_{n+1}$ is the same set as the set of possible integer values this expression takes as the x_i range over integers. The inductive hypothesis tells us that $a_1x_1 + \ldots + a_nx_n$ ranges over all multiples of $\gcd(a_1, \ldots, a_n)$ as $x_1, \ldots, x_n$ vary. Therefore, $a_1x_1 + \ldots + a_nx_n + a_{n+1}x_{n+1} = d$ has a solution exactly when the equation $\gcd(a_1, \ldots, a_n)x' + a_{n+1}x_{n+1} = d$ has a solution. (If this is hard to see, notice that if $a_1x_1+\ldots+a_nx_n+a_{n+1}x_{n+1} = d$ is true, then $a_1x_1 + \ldots + a_nx_n = \gcd(a_1, \ldots, a_n)x'$ for some integer x', and conversely, if $\gcd(a_1, \ldots, a_n)x' + a_{n+1}x_{n+1} = d$ is true, then $\gcd(a_1, \ldots, a_n)x' = a_1x_1 + \ldots + a_nx_n$ for some $x_1, \ldots, x_n$.)

But we know that this new equation, which only has the two variables x', x_{n+1}, has solutions if and only if $\gcd(\gcd(a_1, \ldots, a_n), a_{n+1})$ divides d. And we know that $\gcd(\gcd(a_1, \ldots, a_n), a_{n+1}) = \gcd(a_1, \ldots, a_n, a_{n+1})$, because $d|(\gcd(a_1, \ldots, a_n), a_{n+1})$ if and only if $d|a_1, \ldots, a_{n+1}$. □

(2) Let $a_1, \ldots, a_n$ be positive integers. Show that $\mathrm{lcm}(a_1, \ldots, a_n) = \mathrm{lcm}(\mathrm{lcm}(a_1, a_2), a_3, \ldots, a_n)$. (This is the mirror of exercise 1.9 in the textbook.)

Solution. We will show that the positive common multiples of $a_1, \ldots, a_n$ are exactly the same as the positive common multiples of $\mathrm{lcm}(a_1, a_2), a_3, \ldots, a_n$. This solves the problem, because then the least element in each of these lists of multiples are the respective lcms in each list, and they are equal if the lists are equal.

Suppose ℓ is a common multiple of $a_1, \ldots, a_n$. Then ℓ is a multiple of a_1, a_2, and by a proposition discussed in class (Exercise 1.14 of the text), ℓ must be a multiple of $\mathrm{lcm}(a_1, a_2)$. And of course ℓ is a multiple of $a_3, \ldots, a_n$ already. So ℓ is a common multiple of $\mathrm{lcm}(a_1, a_2), a_3, \ldots, a_n$. Conversely, if ℓ is a multiple of $\mathrm{lcm}(a_1, a_2), a_3, \ldots, a_n$, then ℓ is a multiple of $\mathrm{lcm}(a_1, a_2)$, so is a multiple of a_1, a_2. And ℓ is already a multiple of $a_3, \ldots, a_n$, so ℓ is a common multiple of $a_1, \ldots, a_n$, as desired. □

(3) Find all integer solutions (x, y) to the equation $192x + 66y = 12$.
Solution. First, we calculate $\gcd(192, 66)$. We can use the Euclidean algorithm:

$$\begin{aligned}192 &= 66(2)+60,\\ 66 &= 60(1)+6,\\ 60 &= 6(10).\end{aligned}$$

So $\gcd(192,66)=6$, and $6|12$, so there are solutions. Let's find a solution to $192x+66y=6$. Reverse substituting the Euclidean divisions above, we obtain

$$\begin{aligned}6 &= 66-60,\\ 6 &= 66-(192-66(2))=66(3)-192.\end{aligned}$$

So $x=-1, y=3$ solves $192x+66y=6$. Multiplying this entire equation by 2, we find that $x=-2, y=6$ solves $192x+66y=12$. So let $x_0=-2, y_0=6$; this is our initial solution to $192x+66y=12$.

The formula (see Theorem 1.13) for the general solutions to this equation are

$$x=x_0+\frac{66}{6}n=-2+11n, y=y_0-\frac{192}{6}n=6-32n,$$

where n is an arbitrary integer. □

(4) The post office in Integerland issues 20 cent and 12 cent stamps. You want to make exactly \$2.72 in postage from these stamps. List all the different ways you can do so, and prove that your answer is correct. (Remember, you can't use a negative number of stamps.)

Solution. We are looking for integer solutions to the equation $20x+12y=272$, where $x,y,\geq 0$. Let's first think about solving this equation with no restrictions on the sign of x,y. Notice that $x=13, y=1$ solves $20x+12y=272$ (you can check this by plugging these in; you can find this by noting that $272-12$ is a multiple of 20). Since $\gcd(20,12)=4$, the general solution to this equation is given by

$$x=13+\frac{12}{4}n=13+3n, y=1-\frac{20}{4}n=1-5n.$$

We now are looking for solutions which satisfy $x,y\geq 0$. Notice that with these equations for x,y, if $y\geq 0$, we must have $n\leq 0$. On the other hand, if $x\geq 0$, we must have $13+3n\geq 0$, or $n\geq -4$. Therefore, the solutions corresponding to $n=0,-1,-2,-3,-4$ yield all the solutions where $x,y\geq 0$. These correspond to $(x,y)=(13,1),(10,6),(7,11),(4,16),(1,21)$. □

(5) (This problem is worth double.) Now suppose Integerland issues stamps in a and b cent denominations, where a,b are relatively prime positive integers both greater than 1. Show that

(a) $ab-a-b>0$.

(b) Show that the equation $ax+by=ab-a-b$ has integer solutions x,y, but no matter how hard you try, you cannot actually make $ab-a-b$ cents worth of postage using stamps of size a,b (this means that you should show that any integer solution x,y of $ax+by=ab-a-b$ satisfies either $x<0$ or $y<0$), and

(c) if d is any integer with $d > ab - a - b$, then you can make d cents worth of postage from some combination of a and b cent stamps.

Solution.

(a) First, notice that $a \neq b$, since $\gcd(a, b) = 1$ and $a, b > 1$. Suppose $a > b$. Then $ab - a - b = a(b-1) - b$. But $b - 1 \geq 1$, since $b > 1$, so $a(b-1) - b \geq a - b > 0$, as desired (we are using the fact that a, b are both positive to ensure the inequality signs do not flip.) If $b > a$, repeat the same argument with the equation $ab - a - b = b(a-1) - a$.

(b) Since $\gcd(a, b) = 1$, and $1|(ab-a-b)$, there are evidently some integer solutions to $ax + by = ab - a - b$. In particular, notice that $x = (b-1), y = -1$ is such a solution. The general solutions of this equation are given by the formulas

$$x = (b-1) + bn, y = -1 - an.$$

If $y \geq 0$, we must have $n < 0$. However, if $n < 0$, then $x < 0$. So there are no integer solutions which are simultaneously non-negative.

(c) Again, we know that $ax + by = d$ has some integer solutions since $\gcd(a, b) = 1$ and $1|d$. Let x_0, y_0 be any of these solutions. The general equation for integer solutions is

$$x = x_0 - bn, y = y_0 + an.$$

We choose n to make x as small as possible without becoming negative. (Concretely, choose $n = \lfloor x_0/b \rfloor$.) Notice that for this choice of n, x satisfies $0 \leq x < b$. That $0 \leq x$ is true is clear from the way we chose n. The reason $x < b$ is because if $x \geq b$, then replacing n with $n + 1$, we find that $x_0 - b(n+1) = x - b \geq 0$ is still the x-coordinate of a pair of integer solutions (x, y) to $ax + by = d$ with $x \geq 0$, contradicting the fact that we chose n to make $x_0 - bn$ as small as possible without being negative. (Notice that this value of x is just the remainder when we divide x_0 by b.)
Because x is an integer, the fact that $0 \leq x < b$ actually implies that $0 \leq x \leq b - 1$. Therefore,

$$ax + by \leq a(b-1) + by.$$

On the other hand, since $d = ax + by$, we have

$$d \leq a(b-1) + by \implies d - a(b-1) \leq by.$$

Since $d - a(b-1) > (ab - a - b) - a(b-1) = -b$, this tells us that

$$-b < by, \text{or } -1 < y.$$

(Again, we use the fact that $b > 0$ to ensure that the inequality does not flip direction when we divide by b.) Since y is an integer, this actually implies that $y \geq 0$. So this pair of (x, y) solves $ax + by = d$, with $x, y \geq 0$. □

(6) We know that if p is a prime, n any positive integer, and $p|a^n$, then $p|a$. Classify all numbers d such that for any positive n, if $d|a^n$, then $d|a$. (You should give a simple description of all d which satisfy this property, prove that all such d do indeed satisfy this property, and then give a counterexample for each d which does not satisfy your description.)

Solution. The d which satisfy the above property are those d which are squarefree; ie, those d which are the product of distinct prime numbers. (An alternate way of saying this is that in the prime factorization of d, the exponents are all equal to 1.)

First, suppose d is squarefree, say $d = p_1 \dots p_k$, where the p_i are distinct primes. Suppose that $d|a^n$. Then $p_i|a^n$, which implies that $p_i|a$ (by Euclid's Lemma). Since this is true for all i, and the p_i are mutually coprime, we can repeatedly apply corollary 1.11a of the text to conclude that $(p_1 \dots p_n) \mid a$. Since $d = p_1 \dots p_n$, this yields the desired conclusion of $d|a$.

Now suppose d is not squarefree, say $d = p_1^{e_1} \dots p_k^{e_k}$ where $e = e_j > 1$, for some j. Then if we let $a = p_1 \dots p_k$ (the so-called *squarefree part* of d), and n any integer larger than all the e_is, then $d|a^n$. Indeed, the exponent of p_i in the factorization of d is e_i, and the exponent of p_i in the factorization of a^n is n, which is larger than e_i by the definition of n. However, $d \nmid a$, because the exponent of p_j in the factorization of d, which is greater than 1, is larger than the exponent of p_j in the factorization of a, which is just 1.

(If the construction of the counterexample is somewhat confusing, numerical examples might help. For instance, if $d = 24 = 2^3 \cdot 3$, we can choose $a = 6$, which is $2^1 \cdot 3^1$, and $n = 3$. Then $24 \mid (6)^3$, but $24 \nmid 6$.) □

(7) Recall that if n is a positive integer, $n! = n(n-1)(n-2)\dots(2)(1)$ is the product of the first n positive integers.

(a) Let m be a positive integer. Show that the number of integers between 1 and n which are divisible by m is equal to $\lfloor n/m \rfloor$, where $\lfloor x \rfloor$ is the largest integer less than or equal to x. For instance, $\lfloor 3 \rfloor = 3$, $\lfloor e \rfloor = 2$, $\lfloor 13/2 \rfloor = 6$.

(b) Let p be a prime. Show that $v_p(n!)$ (that is, the exponent of the highest power of p dividing $n!$) is given by the formula

$$v_p(n!) = \sum_{k=1}^{\infty} \left\lfloor \frac{n}{p^k} \right\rfloor = \left\lfloor \frac{n}{p^1} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \dots$$

Solution.

(a) Let's count the number of multiples of m between 1 and n. These multiples are $m, 2m, \dots, km$, for some integer k, which satisfies the property that $km \leq n < (k+1)m$. But notice that this is exactly the definition of $\lfloor n/m \rfloor$, since k is the unique integer which satisfies $k \leq n/m < (k+1)$, and this integer k is precisely $\lfloor n/m \rfloor$.

(b) We know that $n! = (1)(2)\dots(n-1)(n)$. Let us count the number of integers between 1 and n (that is, the number of terms in this product) which are divisible by p^e. By the previous part, this is exactly $\lfloor n/p^e \rfloor$.
We know that $v_p(n!) = \sum_{i=1}^{n} v_p(i)$; this is just an expression of the fact that when we multiply two numbers together, the corresponding exponents in their prime factorizations are summed together. The numbers i, with $1 \leq i \leq n$, satisfying $v_p(i) = 0$, are those numbers from 1 to n not divisible by p.
The numbers i with $1 \leq i \leq n$ satisfying $v_p(i) = e$ are precisely those numbers from 1 to n divisible by p^e but not by p^{e+1}. There are $\lfloor n/p^e \rfloor - \lfloor n/p^{e+1} \rfloor$ such numbers. Therefore,

$$v_p(n!) = \sum_{i=1}^{n} v_p(i) = 1\left(\left\lfloor \frac{n}{p^1} \right\rfloor - \left\lfloor \frac{n}{p^2} \right\rfloor\right) + 2\left(\left\lfloor \frac{n}{p^2} \right\rfloor - \left\lfloor \frac{n}{p^3} \right\rfloor\right) + \dots.$$

This is actually a finite sum, since eventually $p^e > n$, and then $\lfloor n/p^e \rfloor = 0$. So this sum is finite, and then expanding each term and then collecting the terms corresponding to each $\lfloor n/p^e \rfloor$ yields the desired formula. □