MATH 521A: Abstract Algebra

Homework 2 Solutions

1. Let $a, b \in \mathbb{N}$, and set $d = \gcd(a, b)$. Prove that $\gcd(\frac{a}{d}, \frac{b}{d}) = 1$.

   There must be $a', b' \in \mathbb{N}$ with $a = da', b = db'$. Suppose that $\gcd(a', b') = k > 1$. Then k is a common divisor of a', b', and there are $a'', b'' \in \mathbb{N}$ with $a' = ka'', b' = kb''$. Substituting, we get $a = (dk)a'', b = (dk)b''$. Now $dk > d$ is a common divisor of a, b, which contradicts the definition of gcd. Hence in fact $k = 1$.

2. Let $a, b, c \in \mathbb{Z}$. Consider the following equation (in variables x, y):

   $$ax + by = c$$

   Prove that this equation has integer solutions, if and only if $\gcd(a, b)|c$.

   Set $d = \gcd(a, b)$. First, if $d|c$, then there is some $k \in \mathbb{N}$ with $c = dk$. We apply Theorem 1.2 to get $u, v \in \mathbb{Z}$ with $au + bv = d$. Multiplying by k, we get $a(uk) + b(vk) = dk = c$. Taking $x = uk, y = vk$, we are done.

   Suppose now that there are x, y satisfying the equation. If $c = 0$ then $d|c$. If $c > 0$ then c is in $\mathrm{PLC}(a, b)$ and hence $d|c$ by the previous homework set. If instead $c < 0$ then we take $x' = -x, y' = -y$, and get $ax' + by' = (-c)$, so $-c$ is in $\mathrm{PLC}(a, b)$. By the previous homework set, $d|(-c)$, and hence $d|c$.

3. Use the Generalized Euclidean Algorithm to find $\gcd(196, 308)$ and also to find integers x, y satisfying $196x + 308y = \gcd(196, 308)$.

   Step 1: $308 = 1 \cdot 196 + 112$ Step 2: $196 = 1 \cdot 112 + 84$ Step 3: $112 = 1 \cdot 84 + 28$ Step 4: $84 = 3 \cdot 28 + 0$. Hence we conclude that $\gcd(196, 308) = 28$. Continuing, Step 5: $28 = 112 - 1 \cdot 84$ Step 6: $28 = 112 - 1 \cdot (196 - 1 \cdot 112) = 2 \cdot 112 - 1 \cdot 196$ Step 7: $28 = 2 \cdot (308 - 1 \cdot 196) - 1 \cdot 196 = 2 \cdot 308 - 3 \cdot 196$. Hence we take $x = -3, y = 2$.

4. Let $a, b \in \mathbb{N}$. Prove that the Euclidean Algorithm will find $\gcd(a, b)$ in at most $\min(a, b)$ steps.

   Suppose $a > b$ for convenience. By the Division Algorithm, the remainder must decrease at every step. Hence the first remainder must be at most $b - 1$, the next at most $b - 2$, etc. Once the remainder is zero the algorithm terminates; this can take at most b steps.

5. Find all primes between 1025 and 1075.

   There are just eight: $1031, 1033, 1039, 1049, 1051, 1061, 1063, 1069$.

6. Let $a, b, n \in \mathbb{N}$. Prove that $a|b$ if and only if $a^n|b^n$.

   One direction is easier: if $a|b$, then for some $c \in \mathbb{N}$, $b = ca$. Raising to the power n, we get $b^n = c^n a^n$, so $a^n|b^n$.

   Suppose now that $a^n|b^n$. For this direction we need the Fundamental Theorem of Arithmetic. Let $p_1, p_2, \ldots, p_k$ be the primes dividing either or both of a, b. We write

$a = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ and $b = p_1^{b_1} p_2^{b_2} \cdots p_k^{b_k}$, for some $a_i, b_i \in \mathbb{N}_0$. Raising to the power n, we get $a^n = p_1^{na_1} p_2^{na_2} \cdots p_k^{na_k}$ and $b^n = p_1^{nb_1} p_2^{nb_2} \cdots p_k^{nb_k}$. Since $a^n | b^n$, we have $na_1 \leq nb_1$, $na_2 \leq nb_2$, $\ldots$, and $na_k \leq nb_k$. Dividing each inequality by n, we get $a_1 \leq b_1$, $a_2 \leq b_2$, $\ldots$, and $a_k \leq b_k$. Hence $a|b$.

7. Let $n, k \in \mathbb{N}$ and let $p \in \mathbb{N}$ be prime. Prove that if $p|n^k$ then $p^k|n^k$.

We need Corollary 1.6, which states that if prime p divides $a_1 a_2 \cdots a_k$, then it must divide at least one of the a_i. Applying this to $a_1 = a_2 = \cdots = a_k = n$, we conclude that $p|n$. Now applying the previous problem, we conclude that $p^k|n^k$.

8. Let $n \in \mathbb{N}$. Prove that n has an odd number of positive factors, if and only if, n is a perfect square.

Consider the set of positive factors of n. We pair them up in the following way. If m is a factor of n, then so is $\frac{n}{m}$, because $m(\frac{n}{m}) = n$. We pair off m with $\frac{n}{m}$. Typically these pairs contain two different numbers. The sole exception is if $m = \frac{n}{m}$, which arises only when $n = m^2$. Hence, if n is not a perfect square, it has an even number of positive factors. If n is a perfect square, it has an even number of factors apart from $\sqrt{n}$, which is one more positive factor, leaving an odd number.

9. Use the Miller-Rabin test on $n = 69$. Either find a witness to its compositeness, or else three potential liars.

We pull out 2's from $69 - 1 = 68 = 2^2 \cdot 17$, so $d = 17$ and $s = 2$. If we choose $a = 2$, we compute $a^d \pmod{n}$ and $a^{2d} \pmod{n}$, getting 41 and 25 respectively. Hence a is a witness to the compositeness of 69.

10. Use the Miller-Rabin test on $n = 66683$. Either find a witness to its compositeness, or else three potential liars.

We pull out 2's from $66682 = 2 \cdot 33341$, so $d = 33341$ and $s = 1$. If we choose $a = 2$, we compute $a^d \pmod{n}$, getting -1. If we choose $a = 3$, we compute $a^d \pmod{n}$, getting 1. If we choose $a = 5$, we compute $a^d \pmod{n}$, getting -1. Hence either n is prime or we have found three liars.
Note: choosing $a = 4$ is not worthwhile, since we know that $4^d = (2^d)^2$.