Math 110A Homework 1

Jiaping Zeng

1/9/2020

1. Let a be any integer and let b and c be positive integers. Suppose that when a is divided by b, the quotient is q, and the remainder is r, so that $a = bq + r$ and $0 \leq r < b$. If ac is divided by bc, show that the quotient is q and the remainder is rc.

   Answer: Since c is a positive integer, we have $a = bq+r \implies ac = (bq+r)c \implies ac = (bc)q+rc$ and $0 \leq r < b \implies 0 \leq rc < bc$. Then by Division Algorithm, the quotient is bc and the remainder is rc.

2. Let n be a positive integer. Prove that a and c leave the same remainder when divided by n if and only if $a - c = nk$ for some integer k.

   Answer:

   $\Rightarrow$: Suppose a and c leave the same remainder when divided by n, we want to show that $a - c = nk$ for some integer k. By Division Algorithm, we have $a = np + r$ and $c = nq + r$ for quotients $p, q \in \mathbb{Z}$ and remainder $r \in \mathbb{Z}$. Then $a - c = np + r - nq - r = n(p - q)$. Since p and q are both integers, so is their difference. So we can let $k = p - q$ and we have $a - c = nk$ for $k \in \mathbb{Z}$.

   $\Leftarrow$: Suppose $a - c = nk$ for some integer k, we want to show that a and c leave the same remainder when divided by n. By Division Algorithm, we have $a = np + r$ and $c = nq + s$ for quotients $p, q \in \mathbb{Z}$ and remainders $r, s \in \mathbb{Z}$ with $0 \leq r < n$ and $0 \leq s < n$. Then by substitution we have $a - c = np + r - nq - s = n(p - q) + (r - s) \implies r - s = (a - c) - n(p - q) \implies r - s = nk - n(p-q) = n(k-p+q)$, i.e. n divides $r - s$. However, since we have $0 \leq r < n$ and $0 \leq s < n$, which implies that $0 \leq r - s < n$, n can only divide $r - s$ if $r - s = 0$, i.e. $r = s$. Therefore a and c leave the same remainder when divided by n.

3. Suppose a, b, q and r are integers such that $a = bq + r$. Prove the following:

   (a) Every common divisor c of a and b is also a common divisor of b and r.

   Answer: Since c divides both a and b, we have $a = cs$ and $b = ct$ for some $s, t \in \mathbb{Z}$. Then by substitution we have $a = bq + r \implies cs = ctq + r \implies r = cs - ctq = c(s - tq)$. Therefore c also divides r and is a common divisor of b and r.

   (b) Every common divisor of b and r is also a common divisor of a and b.

   Answer: Let m be an arbitrary common divisor of b and r, then $b = mj$ and $r = mk$ for some $j, k \in \mathbb{Z}$. Then by substitution we have $a = bq + r \implies a = mjq + mk = m(jq + k)$. Therefore m also divides a and is a common divisor of a and b.

(c) $(a, b) = (b, r)$.

Answer: By parts (a) and (b), every common divisor of a and b is a common divisor of b and r, and every common divisor of b and r is a common divisor of a and b. Therefore a, b and b, r share the same common divisors and must therefore have the same greatest common divisor, i.e. $(a, b) = (b, r)$.

4. Use the Euclidean algorithm (see Exercise 1.2.15) to compute the gcd (123,90), and find integers u and v with $(123, 90) = 123u + 90v$. Show your work.

Answer: Using the Euclidean algorithm, we have the following:

$123 = 90 \cdot 1 + 33, 0 \leq 33 < 90$

$90 = 33 \cdot 2 + 24, 0 \leq 66 < 90$

$33 = 24 \cdot 1 + 9, 0 \leq 24 < 33$

$24 = 9 \cdot 2 + 6, 0 \leq 6 < 9$

$9 = 6 \cdot 1 + 3, 0 \leq 3 < 6$

$6 = 3 \cdot 2 + 0$

Therefore $(123, 90) = 3$.

5. (a) If $(a, c) = 1$ and $(b, c) = 1$, prove that $(ab, c) = 1$.

Answer: Since $(a, c) = 1$, we must have $au_1 + cv_1 = 1$ for some $u_1, v_1 \in \mathbb{Z}$. Similarly, we also must have $bu_2 + cv_2 = 1$ for some $u_2, v_2 \in \mathbb{Z}$. Upon multiplying the two equations, we have $(au_1 + cv_1)(bu_2 + cv_2) = 1 \implies abu_1u_2 + acu_1v_2 + bcu_2v_1 + c^2v_1v_2 = 1 \implies ab(u_1u_2) + c(au_1v_2 + bu_2v_1 + cv_1v_2) = 1$. Now suppose $(ab, c) = d$, then we must have $ab = dm$ and $c = dn$ for some $m, n \in \mathbb{Z}$. By substitution we have $dm(u_1u_2) + dn(au_1v_2 + bu_2v_1 + cv_1v_2) = 1 \implies d|1$. Therefore $d = (ab, c) = 1$.

(b) Use induction and part (a) to show that if $(a, b) = 1$ then $(a, b^n) = 1$ for all integers $n \geq 1$.

Answer: By induction on n:

Base case: $n = 1$; we want to show that $(a, b) = 1$, which is true by our assumption.

Inductive step: Suppose that $(a, b) = 1 \implies (a, b^n) = 1$, we want to show that $(a, b^{n+1}) = 1$ also. First we note that $(m, n) = (n, m)$ trivially, which lets us swap the variables when using part (a). Now we apply part (a) which gives us $(a, b^n \cdot b) = 1 \implies (a, b^{n+1}) = 1$.

Therefore $(a, b) = 1 \implies (a, b^n) = 1$ by induction.

6. Let $a, b, c \in \mathbb{Z}$. Prove that the equation $ax + by = c$ has integer solutions if and only if $(a, b)|c$.

Answer: Let $d = (a, b)$, then we must have $au + bv = d$ for some $u, v \in \mathbb{Z}$. In addition, since $d|a$ and $d|b$, we also have $a = dm$ and $b = dn$ for some $m, n \in \mathbb{Z}$.

$\Rightarrow$: Suppose $ax + by = c$ has integer solutions, i.e. $x, y \in \mathbb{Z}$, we want to show that $d|c$. By substitution we have $dmx + dny = c \implies d(mx + ny) = c$, which implies that $d|c$.

$\Leftarrow$: Suppose that $d|c$, we want to show that $ax + by = c$ has integer solutions. Since $d|c$, there must exist some $k \in \mathbb{Z}$ such that $c = dk$. By substitution we have $ax + by = dk \implies ax + by = (au + bv)k \implies ax + by = auk + bvk$. Then we can take $x = uk$ and $y = vk$; since u, v, k are all integers, so are x and y.

7. Suppose that $a = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}$ where $p_1, p_2, \ldots, p_k$ are distinct positive primes and each $r_i \geq 0$. Find a formula for the number of positive divisors of a, in terms of the exponents r_i.

   Answer: To construct a positive divisor, we can "choose" an exponent for each p_i and multiply the result together. Note that we can choose from 0 to r_i for each p_i, giving us $r_i + 1$ choices. Therefore, we have $\prod_k (r_i + 1) = k \prod_k r_i$ possible positive divisors.

8. For any integer $n > 0$, prove that $a|b$ if and only if $a^n|b^n$.

   Answer:

   $\Rightarrow$: Suppose that $a|b$, we want to show that $a^n|b^n$. Since $a|b$, there must exist some $m \in \mathbb{Z}$ such that $b = ma$. Since $n > 0$, we have $b^n = (ma)^n \implies b^n = m^n a^n$, where $m^n \in \mathbb{Z}$. Therefore $a^n|b^n$.

   $\Leftarrow$: Suppose that $a^n|b^n$, we want to show that $a|b$. By prime factorization, we have $a = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}$ and $b = p_1^{s_1} p_2^{s_2} \cdots p_k^{s_k}$, where $p_1, p_2, \ldots, p_k$ are distinct positive primes and each $r_i, s_i \geq 0$. Then we also have $a^n = p_1^{nr_1} p_2^{nr_2} \cdots p_k^{nr_k}$ and $b^n = p_1^{ns_1} p_2^{ns_2} \cdots p_k^{ns_k}$ by substitution. Since $a^n|b^n$, we must have $ns_i \geq nr_i$ for each i; then since $n \geq 1$, we also have $s_i \geq r_i$ for each i, i.e. $s_i = r_i + t_i$ where $t_i \geq 0$. Again by substitution we have $b = p_1^{s_1} p_2^{s_2} \cdots p_k^{s_k} = (p_1^{t_1} p_2^{t_2} \cdots p_k^{t_k}) \cdot (p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}) = (p_1^{t_1} p_2^{t_2} \cdots p_k^{t_k})a$. Since $(p_1^{t_1} p_2^{t_2} \cdots p_k^{t_k}) \in \mathbb{Z}$, a divides b by definition.

9. For any integers m and n with $0 \leq m \leq n$, let $\binom{n}{m} = \dfrac{n!}{m!(n-m)!}$. Recall that these are the *binomial coefficients* in the binomial theorem:

$$(a + b)^n = \sum_{m=0}^{n} \binom{n}{m} a^m b^{n-m}.$$

   It is know that $\binom{n}{m}$ is an integer. Let p be a prime and let k be an integer with $1 \leq k \leq p - 1$. Prove that p divides $\binom{p}{k}$.

   Answer: We have $\binom{p}{k} = \dfrac{p!}{k!(p-k)!} = p \cdot \dfrac{(p-1)!}{k!(p-k)!}$. Since p is prime and the denominator is the product of integers strictly less than p, by prime factorization there is no prime factor in $k!(p-k)!$ that divides p. Then for $\binom{p}{k}$ to be an integer as given, we must have $k!(p-k)!|(p-1)!$, i.e. $\dfrac{(p-1)!}{k!(p-k)!} \in \mathbb{Z}$. Therefore p divides $\binom{p}{k}$ by definition.