

Math 113 Homework # 1, selected solutions

2. In the following, (a, b) , (c, d) , etc. will always denote pairs of integers where the second integer is assumed to be nonzero.

(a) *Reflexive:* $(a, b) \sim (a, b)$ because $ab = ba$ since multiplication of integers is commutative.

Symmetric: If $(a, b) \sim (c, d)$, i.e. $ad = bc$, then since multiplication of integers is commutative, $cb = da$, so $(c, d) \sim (a, b)$.

Transitive: Suppose $(a, b) \sim (c, d)$ and $(c, d) \sim (e, f)$, i.e. $ad = bc$ and $cf = de$. We need to show that $(a, b) \sim (e, f)$, i.e. $af = be$. Multiplying the two equations we know by f and b respectively, we get $adf = bcf$ and $bcf = bde$, so $adf = bde$. Since d is assumed nonzero, it follows that $af = be$.

(b) Suppose that $(a, b) \sim (a', b')$ and $(c, d) \sim (c', d')$. To prove that our definition of addition is well-defined, we must check that

$$(ad + bc, bd) \sim (a'd' + b'c', b'd'),$$

i.e. $(ad + bc)(b'd') = (bd)(a'd' + b'c')$, or multiplying out,

$$adb'd' + bcb'd' = bda'd' + bdb'c'.$$

Since $(a, b) \sim (a', b')$ we can replace ab' by $a'b$ in the first term on the left, and since $(c, d) \sim (c', d')$ we can replace cd' by $c'd$ in the second term on the left. Then everything cancels, so the equation we are trying to prove is true.

Strictly speaking, we should also check that the addition operation sends $S \times S$ to S , i.e. $(ad + bc, bd) \in S$. But this is clear because $bd \neq 0$ since b and d are assumed nonzero.

The proof that multiplication is well defined is similar and we omit it.

3. (a) Let S denote the set of common divisors of a and b , and let T denote the set of common divisors of b and r . I claim that $S = T$. The equation $a = qb + r$ implies that any divisor of b and r also divides a , so $T \subset S$. Likewise the equation $r = a - qb$ implies that any divisor of a and b also divides r , so $S \subset T$. Thus $S = T$. In particular the largest element of S is the same as the largest element of T , and this is what we were supposed to prove.

- (b) We can assume that $a > 0$ (because if $a = 0$ then $\gcd(a, b) = b$ so we can just take $x = 0, y = 1$, and if $a < 0$ then we can just switch the signs of a and x). So we need to prove that if a and b are positive integers, then there exist integers x, y such that $ax + by = \gcd(a, b)$. We will prove this by (strong) induction on $\max(a, b)$. So we can assume that the statement is true for all pairs of positive integers (a', b') with $\max(a', b') < \max(a, b)$. Since the order of a and b is irrelevant, we can assume without loss of generality that $a \geq b$. By the division theorem we can write $a = qb + r$ where q and r are integers with $0 \leq r < b$. We consider two cases. Case 1: $r = 0$. Then a is a multiple of b , so $\gcd(a, b) = b$, and we can take $x = 0, y = 1$. Case 2: $0 < r < b$. Then $\max(b, r) = b < a$ (we can't have $a = b$ because then we would be in Case 1), so by inductive hypothesis there exist integers x', y' with $bx' + ry' = \gcd(b, r)$. It follows from part (a) that $bx' + ry' = \gcd(a, b)$. Substituting $r = a - qb$ into this equation, we get $\gcd(a, b) = bx' + (a - qb)y' = ay' + (x' - qy')b$, so we can take $x = y', y = x' - qy'$.

Note that a proof by induction that something exists generally corresponds to a recursive algorithm for finding it. The above proof corresponds to the procedure of “working backwards through the Euclidean algorithm” which we discussed in class.

5. (a) We use induction on n . So we can assume that every positive integer $n' < n$ has a binary expansion. By the division theorem there are integers q and r with $n = 2q + r$ and $r \in \{0, 1\}$. We consider two cases. Case 1: $q = 0$. Then $n = 1$ and it has the binary expansion $n = 2^0$. Case 2: $q > 0$. Then q is a positive integer and the equation $n = 2q + r$ implies that $q < n$. So by inductive hypothesis q has a binary expansion $q = 2^{k_1} + \dots + 2^{k_m}$ where k_1, \dots, k_m are distinct nonnegative integers. Then $2q = 2^{k_1+1} + \dots + 2^{k_m+1}$, and $k_1 + 1, \dots, k_m + 1$ are distinct positive integers. If $r = 0$ then this is a binary expansion of n , and if $r = 1$ then a binary expansion of n is obtained from this by adding 2^0 (and 0 is distinct from $k_1 + 1, \dots, k_m + 1$ since the latter are positive integers).
- (b) Suppose n has two different binary expansions. There is at least one integer m such that 2^m appears in one of the binary expansions but not the other. Let m be the largest such integer. Then

subtracting the two binary expansions gives an equation of the form

$$2^m = \sum_{i=0}^{m-1} a_i 2^i$$

where $a_i \in \{-1, 0, 1\}$. But the right hand side is bounded from above by

$$\left| \sum_{i=0}^{m-1} a_i 2^i \right| \leq \sum_{i=0}^{m-1} |a_i 2^i| \leq \sum_{i=0}^{m-1} 2^i = 2^m - 1,$$

a contradiction.

6. (2a) should be straightforward. (2b) should also be straightforward, provided that you know what you are supposed to do. Please be sure you know what it means to prove that a function defined on a set of equivalence classes is well-defined. I think (3a) is not so hard. (3b) is trickier (and one has to be careful about some cases before getting to the heart of the matter). Anyway please be sure you understand how to translate a recursive algorithm into a proof by induction, and vice-versa. (5a) is probably not too hard if you follow the hint, but (5b) requires some creativity (and like most problems it has more than one solution). Note that similar arguments show that every positive integer has a unique base 10 expansion; do you see why?