

Math 113 Homework # 2, selected solutions

1. 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.

To be careful, 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.

2. (a) *Base case:* When $k = 1$, this is true since $2^1 = 2 > 1$.

Inductive step: Suppose k is a positive integer and $2^k > k$. We need to show that $2^{k+1} > k + 1$. There are a number of ways to do this. For example, $2^{k+1} = 2 \cdot 2^k$. By inductive hypothesis, $2 \cdot 2^k > 2k$. And $2k = k + k \geq k + 1$ since $k \geq 1$.

Parts (b) and (c) require a bit of creativity, and there are many possible solutions, of which I have given two each.

- (b) *First proof:* We use strong induction. Let n be a positive integer and assume that every positive integer less than n has a binary expansion. Let $S = \{a \in \mathbb{N} \mid 2^a \leq n\}$. This set is nonempty (since it contains 0) and has an upper bound (namely n , by part (a)). By the well-ordering principle, S has a largest element, call it a . Let $n' = n - 2^a$. If $n' = 0$ then 2^a is our binary expansion of n . Otherwise $n' > 0$, so by inductive hypothesis, n' has a binary expansion. Then adding 2^a to the binary expansion of n' gives a binary expansion of n . We have to check that this is really a binary expansion, i.e. that this is a sum of *distinct* powers of two. The exponents in the expansion of n' are distinct by the definition of binary expansion. Also note that $n' < 2^a$ since otherwise $a+1 \in S$. Hence our expansion of n' cannot contain 2^a . Thus the exponents in our expansion of n are distinct.

Second proof: We use strong induction again. Let n be a positive integer and assume that every positive integer less than n has a binary expansion. By the division theorem we can write $n = 2q + r$ where q is an integer and $r \in \{0, 1\}$. Since $n > 0$, it follows that q is a nonnegative integer. If $q = 0$ then $n = 1$ and a binary expansion of n is 2^0 . Otherwise $q > 0$, and it follows from $n = 2q + r$ that $q < n$. By inductive hypothesis, q has a binary expansion. We now obtain a binary expansion of n by increasing each exponent in the binary expansion of q by one, and adding 2^0 if $r = 1$. The exponents in this expansion of n are distinct because we know that the exponents for q are distinct; and after shifting these exponents by one, they are still distinct and all positive, so adding 2^0 does not create any overlap.

- (c) *First proof:* Suppose we have two different binary expansions of the same integer. Let k be the largest integer such that the coefficients of 2^k in the two binary expansions are different. Subtracting the two binary expansions, we obtain an equation of the form

$$\epsilon_0 2^0 + \epsilon_1 2^1 + \cdots + \epsilon_{k-1} 2^{k-1} = 2^k$$

where $\epsilon_i \in \{-1, 0, 1\}$. Taking the absolute value of both sides we obtain

$$|\epsilon_0 2^0 + \epsilon_1 2^1 + \cdots + \epsilon_{k-1} 2^{k-1}| = 2^k.$$

But this is impossible because by an exercise on HW#1,

$$\begin{aligned} |\epsilon_0 2^0 + \epsilon_1 2^1 + \cdots + \epsilon_{k-1} 2^{k-1}| &\leq |\epsilon_0 2^0| + |\epsilon_1 2^1| + \cdots + |\epsilon_{k-1} 2^{k-1}| \\ &\leq 2^0 + 2^1 + \cdots + 2^{k-1} \\ &= 2^k - 1 \\ &< 2^k. \end{aligned}$$

Seond proof: If a particular positive integer contains two different binary expansions, then there is some upper bound, call it $k-1$, on the exponents in the two binary expansions. Hence it is enough to show that a binary expansion of a given positive integer containing no powers of 2 greater than 2^{k-1} is unique if it exists. Let $S = \{(a_0, a_1, \dots, a_{k-1}) \mid a_i \in \{0, 1\}\}$. Define

$$f : S \rightarrow \{0, 1, \dots, 2^k - 1\}$$

by $f(a_0, a_1, \dots, a_{k-1}) = a_0 2^0 + a_1 2^1 + \cdots + a_{k-1} 2^{k-1}$. Note that this is in $\{0, 1, \dots, 2^k - 1\}$ by the calculation above. Now f is surjective, because $0 = f(0, \dots, 0)$, and we know from the existence proof that every integer from 1 to $2^k - 1$ has a binary expansion, and this cannot contain any powers of 2 greater than 2^{k-1} . Since f is surjective and $|S| = 2^k = |\{0, 1, \dots, 2^k - 1\}|$, it follows that f is injective, and this implies our uniqueness statement.

3. (a) Suppose c is an integer such that $a/b = c$. Then $a = bc$, so $b|a$, so $\gcd(a, b) = b$. This contradicts our assumptions that $\gcd(a, b) = 1$ and $b > 1$.
- (b) Suppose $\gcd(a, b) = 1$. Then $\gcd(a^2, b^2) = 1$, because if a^2 and b^2 have a common factor $d > 1$, then they have a prime common factor p (since d has a prime factorization). Since $p|a^2$, by a result proved in class, $p|a$ or $p|a$, i.e. $p|a$. Likewise $p|b$. So $\gcd(a, b) \geq p$, a contradiction.
- (c) (\Rightarrow) Suppose $\sqrt{n} = a/b$ where a and b are integers with $b \neq 0$. Without loss of generality, $\gcd(a, b) = 1$, since we can cancel any common factors. Then $\gcd(a^2, b^2) = 1$ by part (b). Since $a^2/b^2 = n \in \mathbb{Z}$, part (a) implies that $b^2 = 1$. Hence $b \in \{1, -1\}$ so $\sqrt{n} \in \mathbb{Z}$. (\Leftarrow) Immediate since $\mathbb{Z} \subset \mathbb{Q}$.

One can also solve problem 3 using unique prime factorization, although this makes the notation a bit more complicated.

4. (a) From the euclidean algorithm we find that $\gcd(83, 157) = 1$. Working backward through the euclidean algorithm, we find that $1 = -37 \cdot 157 + 70 \cdot 83$. Hence $x = 70$ solves the equation $83x \equiv 1 \pmod{157}$. Thus $x = 280$ solves the equation $83x \equiv 4 \pmod{157}$. To simplify this we can also subtract 157 to get $x = 123$.
- (b) By the Euclidean algorithm we find that $\gcd(1001, 611) = 13$. Then the equation $1001x \equiv 131 \pmod{611}$ has no integer solution, because if it did then 131 would be a multiple of $\gcd(1001, 611) = 13$, but it is not since $131 \equiv 1 \pmod{13}$.