Math 502: Abstract Algebra
Homework 1

Lawrence Tyler Rush
<me@tylerlogic.com>

February 1, 2014
http://coursework.tylerlogic.com/courses/upenn/math502/homework01

1

First, a helpful Lemma. Let S be defined as in the problem's specification.

Lemma 1.1. *The set S is $n\mathbb{Z}$ for some $n \in \mathbb{N}_{>0}$.*

Proof. First note that S has positive elements, for if $s \in S$ and $s \neq 0$ (such an s exists since S has at least two different elements), then either s is positive or $s - 2s$ is; the latter being guaranteed to be in S due to the closure of addition and subtraction.

As a subset of the well-ordered set $\mathbb{N}$, the set $S \cap \mathbb{N} - \{0\}$, must have a least element, call it n. Certainly all integer multiples of n are in S as S is closed under addition and subtraction. So in the least,

$$n\mathbb{Z} \subseteq S \tag{1.1}$$

Assume for later contradiction that there is an $a \in S$ for which $n \not| a$. Then the division algorithm, since $n \neq 0$, yields the existence of $q, r \in \mathbb{Z}$ with $0 \leq r < |n|$ such that $a = qn + r$. Therefore $r = a - qn \in S$ by the closure of addition and subtraction on S. Since a was assumed to not be a multiple of n, then $0 < r < |n|$, but this contradicts the fact that n is the least element of $S \cap \mathbb{N} - \{0\}$. Thus, no such a exists, moreover all elements of S are multiples of n. Hence combining this with equation 1.1 leaves us with $S = n\mathbb{Z}$. $\square$

(a)

Given that $S = n\mathbb{Z}$ by Lemma 1.1, define $f : \mathbb{N} \to \mathbb{N} \cap S$ by

$$f(m) = mn$$

This is surjective since any element of $\mathbb{N} \cap S$ has the form mn and thus f will map m to it. The map is injective because if $f(m) = f(m')$ for $m, m' \in \mathbb{N}$, then $nm = nm'$ and thus $m = m'$. So f is a bijection.

Because multiplication by a nonzero natural number preserves order, then f is an order-preserving map as it simply multiplies its input by the nonzero natural number n.

Finally to prove uniqueness, let $g : \mathbb{N} \to \mathbb{N} \cap S$ be an order-preserving bijection. We first note that $g(0) = 0$ because 0 is the least element of both $\mathbb{N}$ and $\mathbb{N} \cap S$; any other output for g would contradict its given order-preservation. Now assume that there exists an N such that for all k with $0 \leq k < N$ we have $g(k) = f(k)$. Define ℓ by $\ell = \min\{j \in S \cap \mathbb{N} \mid j \geq f(N) = mN\}$, remembering that $S = n\mathbb{Z}$. We know ℓ exists since $S \cap \mathbb{N}$ is a subset of the well-ordered set $\mathbb{N}$. Thus $f(k) = mk < \ell$ for all k such that $0 \leq k < N$, and therefore since f is an order-preserving bijection, $f(N) = \ell$. However, the inductive hypothesis implies that g, being an order-preserving bijection, must also have that $g(N) = \ell$. Hence g and f are one in the same.

(b)

The fact that every element of S is a multiple of $f(1)$ follows directory from Lemma 1.1, the fact that n generates $n\mathbb{Z}$, and the construction of f, namely $f(1) = n$.

(c)

Let G be a cyclic group with subgroup H and generator g. If H is trivially $\{1\}$, then we are done, as 1 generates H.

So assume that H has at least two distinct elements. Define $S = \{n \mid g^n \in H\}$. The set S then also has at least two different elements. Now for $n, m \in S$ we have that $g^n, g^m \in H$ which implies that $g^n g^m = g^{n+m} \in H$ as H is a group. Hence $n + m \in S$ implying the closure of S under addition. Also since H is a group, $(g^m)^{-1} = g^{-m} \in H$ informing us that $n - m \in S$. Hence S is closed under subtraction. In summary, S is a set with at least two different elements which is closed under addition and subtraction.

Thus by parts (a) and (b) of this problem, we have a unique order-preserving map, $f : \mathbb{N} \to S \cap \mathbb{N}$, for which every element of S is an integer multiple of $f(1)$. In other words, for every $g^n \in H$, there is some integer a such that $g^n = g^{af(1)} = \left(g^{f(1)}\right)^a$. Hence $g^{f(1)}$ generates H.

2

(a)

Let $a, b \in \mathbb{Z}$ be nonzero, and $S \subset \mathbb{Z}$ be the set $\{ar + bs \mid r, s \in \mathbb{Z}\}$. If $a = b$, then the existence of the greatest common divisor of a, a is trivial since the a would be the integer such that any other integer which divides a also divides a.

So let's proceed assuming that $a \neq b$. With this, we know that S has at least two elements, thereby allowing us to make use of the problem 1. So let $f\mathbb{N} \to \mathbb{N} \cap S$ be the unique order-preserving bijection, and define c to be $f(1)$. So for any d that divides a and b, d will also divide every element of S. This will include c since part (b) of problem 1 states that c generates all of S and c is therefore contained in S. So d divides c.

Relation of $gcd(a, b)$ to S The greatest common divisor of a, b is the value c such that c generates $S = \langle a, b \rangle$.

(b)

Let a, b be relatively prime non-zero integers and c an integer such that $a|bc$. Let $as + cr \in \langle a, c \rangle$ for some $s, r \in \mathbb{Z}$. Since a and b are relatively prime, their greatest common divisor is 1, meaning that $\langle a, b \rangle = \langle 1 \rangle = \mathbb{Z}$. Therefore $r \in \langle a, b \rangle$. However, for $n, m \in \mathbb{Z}$ such that $an + bm = r$, this implies that $as + cr = as + c(an + bm) = as + can + cbm$. Thus a divides $as + cr$, since $a|bc$, and therefore every element of $\langle a, c \rangle$, including $a(0) + c(1) = c$ is divisible by a.

(c)

We will define a prime according to Jacobson [Jac09, pg. 22] as an integer $p \neq 0, \pm 1$ with $\pm p$ and ± 1 being its only divisors.

Every nonzero integer can be decomposed into $\pm 1 p_1^{e_1} \cdots p_m^{e+m}$ We will first prove this for positive integers, then for negative ones.

As a base case we have that for 1 or any positive prime p, the decomposition is 1 and p, respectively. So let $n \in \mathbb{N}$ be composite and assume that all natural numbers less than n can be decomposed as per above. Then we can find positive integers $q, r < n$ such that $qr = n$. By the inductive hypothesis, then q and r can be decomposed into $\pm$ a product powers of primes. Hence so can n, namely the decomposition produced by the product of the decomposition of q and r.

As for a negative integer, m, the above proof for decomposition of positive integers informs us that there is such a decomposition for $|m|$, and thus simply negating the decomposition yields a decomposition for m.

The decomposition is unique. As a base case we have that for 1 or any positive prime p, the decomposition 1 and p, respectively, are unique. So let $n \in \mathbb{N}$ be composite and assume that all natural numbers less than n can be uniquely decomposed. Let $p_1^{e_1} \cdots p_a^{e_a}$ and $q_1^{f_1} \cdots q_b^{f_b}$ be decompositions of n. Therefore p_1 must divide $q_1^{f_1} \cdots q_b^{f_b}$ since both decompositions are equal, in other words, there is some q_i equal to p_1. Thus $p_1^{e_1 - 1} \cdots p_a^{e_a}$ and $q_1^{f_1} \cdots q_i^{f_i - 1} \cdots q_b^{f_b}$ are equal, but these integers are less than n, which our inductive hypothesis tells us that their prime decompositions are unique. Therefore their multiplication by $p_1 = q_i$ will be unique decompositions of n.

As for a negative integer, m, the above proof for unique decomposition of positive integers informs us that there is such a unique positive decomposition for $|m|$, and thus simply negating the it yields a unique decomposition for m.[1]

[1] Inspiration for this proof drawn from [Jac09, pg. 22]

3

Suppose that m, n are integers that are relatively prime. From problem two, we know that there exist integers u, v such that $um + vn = 1$. From this we obtain that $um + vn \equiv 1 \bmod n$, but since vn is a multiple of n this yields $um \equiv 1 \bmod n$. Similarly we obtain $vn \equiv 1 \bmod m$. These two equations in turn give us that for some integers a, b,

$$bum \equiv b \bmod n \qquad \text{and} \qquad avn \equiv a \bmod m \tag{3.2}$$

As multiples of m and n, respectively, bum and avn have that

$$bum \equiv 0 \bmod m \qquad \text{and} \qquad avn \equiv 0 \bmod n$$

which when combined with Equation 3.2, yields

$$avn + bum \equiv a \bmod m \text{ and } avn + bum \equiv b \bmod n$$

Thus the desired formula for c is $c = avn + bum$

4

(a)

Let $a \in \mathbb{N}$ be a $n+1$ decimal digit number. Let the decimal digits of a be represented by $d_0, d_1, \dots, d_n$ where each d_i is in $\{0, 1, \dots, 9\}$ and d_0 corresponds to the lowest magnitude digit, and d_n, the highest. Then we have that

$$a = \sum_{i=0}^{n} d_i 10^i$$

In class we saw that the canonical addition and multiplication operations in $\mathbb{Z}/9\mathbb{Z}$ are compatible with the addition and multiplication operations of the integers. This yields to us

$$a \equiv \left(\sum_{i=0}^{n} d_i 10^i\right) \bmod 9 = \sum_{i=0}^{n} (d_i \bmod 9)\left(10^i \bmod 9\right) = \sum_{i=0}^{n} (d_i \bmod 9)\underbrace{(10 \bmod 9)\cdots(10 \bmod 9)}_{i \text{ times}}$$

however, $1 \equiv 10 \bmod 9$, leaving us with

$$a \equiv \sum_{i=0}^{n} (d_i \bmod 9) = \left(\sum_{i=0}^{n} d_i\right) \bmod 9$$

again using the compatibility of addition in $\mathbb{Z}/9\mathbb{Z}$ with integer addition.

(b)

Let $a \in \mathbb{N}$ be a $n+1$ decimal digit number. Let the decimal digits of a be represented by $d_0, d_1, \dots, d_n$ where each d_i is in $\{0, 1, \dots, 9\}$ and d_0 corresponds to the lowest magnitude digit, and d_n, the highest.

Formula for 11 We can see that 10 is a unit of $\mathbb{Z}/11\mathbb{Z}$ with order 2 in $(\mathbb{Z}/11\mathbb{Z})^\times$. Therefore $10^{2i} \equiv 10 \bmod 11$ and $10^{2i+1} \equiv 1 \bmod 11$ for integer i. We can also say that $d_i = 0$ when $i > n$, and because of it, we can write

$$a = \sum_{i=0}^{n} d_i 10^i = \sum_{i=0}^{n} d_{2i} 10^{2i} + \sum_{i=0}^{n} d_{2i+1} 10^{2i+1}$$

which implies

$$a \equiv \left(\sum_{i=0}^{n} d_{2i} 10^{2i} + \sum_{i=0}^{n} d_{2i+1} 10^{2i+1}\right) \bmod 11 \equiv \sum_{i=0}^{n} d_{2i}\left(10^{2i} \bmod 11\right) + \sum_{i=0}^{n} d_{2i+1}\left(10^{2i+1} \bmod 11\right) \equiv 10\sum_{i=0}^{n} d_{2i} + \sum_{i=0}^{n} d_{2i+1}$$

Formula for 7 Similar to the above method for 11, 10 is a unit of $\mathbb{Z}/7\mathbb{Z}$ with order 6 in $(\mathbb{Z}/7\mathbb{Z})^\times$. Therefore

$$\begin{aligned} 10^0 &\equiv 1 \bmod 7 \\ 10^1 &\equiv 3 \bmod 7 \\ 10^2 &\equiv 2 \bmod 7 \\ 10^3 &\equiv 6 \bmod 7 \\ 10^4 &\equiv 4 \bmod 7 \\ 10^5 &\equiv 5 \bmod 7 \end{aligned}$$

We can again also say that $d_i = 0$ when $i > n$, and because of it, we can write

$$a = \sum_{i=0}^{n} d_i 10^i = \sum_{i=0}^{n} d_{6i} 10^{6i} + \sum_{i=0}^{n} d_{6i+1} 10^{6i+1} + \sum_{i=0}^{n} d_{6i+2} 10^{6i+2} + \sum_{i=0}^{n} d_{6i+3} 10^{6i+3} + \sum_{i=0}^{n} d_{6i+4} 10^{6i+4} + \sum_{i=0}^{n} d_{6i+5} 10^{6i+5}$$

which results in the following after modding by 7

$$a = \sum_{i=0}^{n} d_{6i} + 3\sum_{i=0}^{n} d_{6i+1} + 2\sum_{i=0}^{n} d_{6i+2} + 6\sum_{i=0}^{n} d_{6i+3} + 4\sum_{i=0}^{n} d_{6i+4} + 5\sum_{i=0}^{n} d_{6i+5}$$

5

(a) Prove Euler's totient function is multiplicative

First, let m and n be coprime integers. Then problem 1 informs use that there are intgers r, s such that $mr + ns = 1$ or in other words $mr = n(-s) + 1$, which implies $mr \equiv 1 \bmod n$. Hence $\overline{m} \in (\mathbb{Z}/n\mathbb{Z})^\times$.

Now let $\overline{m} \in (\mathbb{Z}/n\mathbb{Z})^\times$. Then there exists some integer r such that $mr \equiv 1 \bmod (n)$. Then problem 1 implies the existence of an s such that $mr = ns + 1$, i.e. $mr + n(-s) = 1$. Hence $\gcd(m, n) = 1$ and therefore m and n are coprime.

Combining these two results implies that an integer m is coprime to an integer n if and only if $\overline{m} \in (\mathbb{Z}/n\mathbb{Z})^\times$. This allots us the following equation

$$\phi(n) = \left|(\mathbb{Z}/n\mathbb{Z})^\times\right| \tag{5.3}$$

The multiplicativity of ϕ According to [Cha13] the Chinese Remainder Theorem tells us that for an integer $n \geq 2$ with prime factorization $n = p_1^{e_1} \cdots p_a^{e_a}$, $\mathbb{Z}/n\mathbb{Z}$ is isomorphic to $(\mathbb{Z}/p_1^{e_1}\mathbb{Z}) \times \cdots \times (\mathbb{Z}/p_a^{e_a}\mathbb{Z})$. This in turn implies $(\mathbb{Z}/n\mathbb{Z})^\times$ is isomorphic to $(\mathbb{Z}/p_1^{e_1}\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/p_a^{e_a}\mathbb{Z})^\times$. Let m and n be coprime with prime factorizations $p_1^{e_1} \cdots p_a^{e_a}$ and $q_1^{f_1} \cdots q_b^{f_b}$, respectively. Therefore the prime factors of their prime factorization have that $p_i \neq q_j$ for each possible i, j. Now according to equation 5.3, $\phi(mn) = |\mathbb{Z}/mn\mathbb{Z}|$, and thus we have the following sequence of equations.

$$\begin{aligned} \phi(mn) &= \left|(\mathbb{Z}/p_1^{e_1}\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/p_a^{e_a}\mathbb{Z})^\times \times (\mathbb{Z}/q_1^{f_1}\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/q_b^{f_b}\mathbb{Z})^\times\right| \\ &= \left|(\mathbb{Z}/p_1^{e_1}\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/p_a^{e_a}\mathbb{Z})^\times\right| \left|\left(\mathbb{Z}/q_1^{f_1}\mathbb{Z}\right)^\times \times \cdots \times \left(\mathbb{Z}/q_b^{f_b}\mathbb{Z}\right)^\times\right| \\ &= \left|(\mathbb{Z}/m\mathbb{Z})^\times\right| \left|(\mathbb{Z}/n\mathbb{Z})^\times\right| \\ &= \phi(m)\phi(n) \end{aligned}$$

(b)

Let's first examine the value of $\phi(p^e)$ for prime p and positive e (note negative e is pointless to consider as it isn't an integer). The value of $\phi(p^e)$ will be the number of integers between 1 and p^e which are coprime to p^e, but the only such integers are the positive multiples of p less than or equal to p^e. There are p^{e-1} of them, namely $p, 2p, 3p, \ldots, (p^{e-1})p$. Hence, because there are p^e postive integers less than or equal to p^e

$$\phi(p^e) = p^e - p^{e-1} = p^{e-1}(p-1) \tag{5.4}$$

Given Equation 5.4 and the fact that ϕ is multiplicative from the previous part of the problem, then for any n with prime decomposition of $p_1^{e_1} p_2^{e_2} \cdots p_m^{e_m}$ where each p_i is distinct, we have the formula

$$\phi(n) = \phi(p_1^{e_1} p_2^{e_2} \cdots p_m^{e_m}) = \phi(p_1^{e_1})\phi(p_2^{e_2}) \cdots \phi(p_m^{e_m}) = p_1^{e_1-1}(p_1-1)p_2^{e_2-1}(p_2-1) \cdots p_m^{e_m-1}(p_m-1)$$

References

[Cha13] Ching-li Chai. Excursion in elementary number theory. `http://www.math.upenn.edu/~chai/502f13/course_notes/nber_thy.pdf`, 2013.

[Jac09] Nathan Jacobson. *Basic Algebra I*. Basic Algebra. Dover Publications, Incorporated, 2009.