MATH 430 Problem Set 3

Qilin Ye

November 4, 2020

Problem 1

Find a minimal subset $S \subset Z$ such that S contains $0, m = 27, n = 18$ and is a group under usual integer addition.

Solution

Since, as a group, S is closed under integer addition, we know that $m - n = 9 \in S$. Note that for all $x, y \in \mathbb{Z}$, we always have

$$xm + yn = 27x + 18y = 9 \cdot 3x + 9 \cdot 2y = 9 \cdot (3x + 2y).$$

Thus any element obtained from a $\mathbb{Z}$-combination of 27 and 18 is an element in the set of multiple of 9's, and the same logic can be applied to any addition of any elements obtained in this way. The set of all multiples of 9 is a subset of $\mathbb{Z}$ satisfying the requirements (0 is a multiple of 9, of course). If we take away any element in this set then we are missing an integer of form $9k$, which can be obtained by adding 9's k times. Hence $S = \{9k \mid k \in \mathbb{Z}\}$ is the minimal subset satisfying the conditions.

Problem 2

Let p be a prime. We call $a \in (\mathbb{Z}/p\mathbb{Z})$ to be a generator if $\{\dots, -a, 0, a + a, a + a + a, \dots\} = (\mathbb{Z}/p\mathbb{Z})$. How many generators does this group have? Explain your answer.

Solution

Clearly $0 \in (\mathbb{Z}/p\mathbb{Z})$ is not a generator since adding 0's always gives 0, not anything else. However, if p is prime, x is a generator for all $1 \leqslant x \leqslant p - 1$.

Proof

Pick an arbitrary $x \in (\mathbb{Z}/p\mathbb{Z})$ with $x > 1$, and we want to show that, for all $y \in (\mathbb{Z}/p\mathbb{Z})$, there exists t such that $\underbrace{x + x + \cdots + x}_{t \text{ times}} = y$. This is equivalent to saying

$$tx \equiv y \pmod{p}$$

Since p is a prime, we know that $\gcd(x, p) = 1$ for all $1 \leqslant x \leqslant p - 1$. Therefore there is a solution to $kx \equiv 1 \pmod{p}$ by Euclid's algorithm and substitution. Then $(ky)x \equiv y \pmod{p}$ and we have found a solution of t. The only exception is when $y = 0$, in which case we can solve it by letting $t = p$. Then $px \equiv 0 \pmod{p}$. With the exception handled, we conclude that, since y is arbitrary, x can generate any element in $(\mathbb{Z}/p\mathbb{Z})$. Hence x is a generator. □

Since x is also arbitrary, we claim that all $x \in [1, p - 1]$ are generators of $(\mathbb{Z}/p\mathbb{Z})$. Therefore this group has $p - 1$ generators.

Problem 3

Given 2 is a generator of $(\mathbb{Z}/29\mathbb{Z})^*$, how many generators does this group have? Given 7 is a generator of $(\mathbb{Z}/229\mathbb{Z})^*$, how many generators does this group have?

Solution

(1) Since 2 generates $(\mathbb{Z}/29\mathbb{Z})^*$, we know that

$$\{\dots, 2^{-2}, 2^{-1}, 1, 2, 2^2, \dots\} = \{1, 2, \dots, 28\},$$

i.e., the set on the LHS permutes the set on the RHS.

First, we claim that $o(2) = 28$. On the one hand, by Lagrange's theorem we immediately know $o(2) \mid |(\mathbb{Z}/29\mathbb{Z})^*| = 28$. On the other hand, if $o(2) < 28$, then the LHS can have at most 27 distinct elements and the equation cannot hold. Hence $o(2) = 28$, i.e., $2^{28} = e$.

Also note that

$$\begin{cases} 2^i 2^j = 2^{i+j} \\ 2^i 2^{28-i} = 2^{28} = e \implies (2^i)^{-1} = 2^{28-i} \end{cases}$$

Now if we only look at the exponents, the two equations give nothing else but the group $(\mathbb{Z}/28\mathbb{Z}, +)$, and the bijective map $f : \mathbb{Z}/28\mathbb{Z} \to (\mathbb{Z}/29\mathbb{Z})^*$ defined by $f(x) = 2^x$ shows that the two groups are isomorphic.

Clearly, as 2 generates $(\mathbb{Z}/29\mathbb{Z})^*$, any other generator (and non-generator) has the form 2^n, and to be a generator, 2^n has to satisfy that, given any b with $0 \leqslant b \leqslant 27$, we can always find an a such that $(2^n)^a = 2^b$ in $\mathbb{Z}/28\mathbb{Z}$. Alternatively, we can write this as

$$an \equiv b \pmod{28}$$

which will always have a solution if and only if $\gcd(n, 28) = 1$. (The "if" part is immediate by applying Euclid's algorithm and solving the equation $b(an) + b(28c) = b(1)$. The "only if" part can be proven by taking the contrapositive: suppose $\gcd(n, 28) = m > 1$, then any $\mathbb{Z}$-combination of n and 28 is still a multiple of m. Hence if $m \nmid b$, it is impossible to find a solution for $an \equiv b \pmod{28}$.)

Therefore, x needs to be coprime with 28 to be a generator of $(\mathbb{Z}/29\mathbb{Z})^*$. Hence there are $\varphi(28) = 28 \cdot (1/2) \cdot (6/7) = 12^\dagger$ such generators.

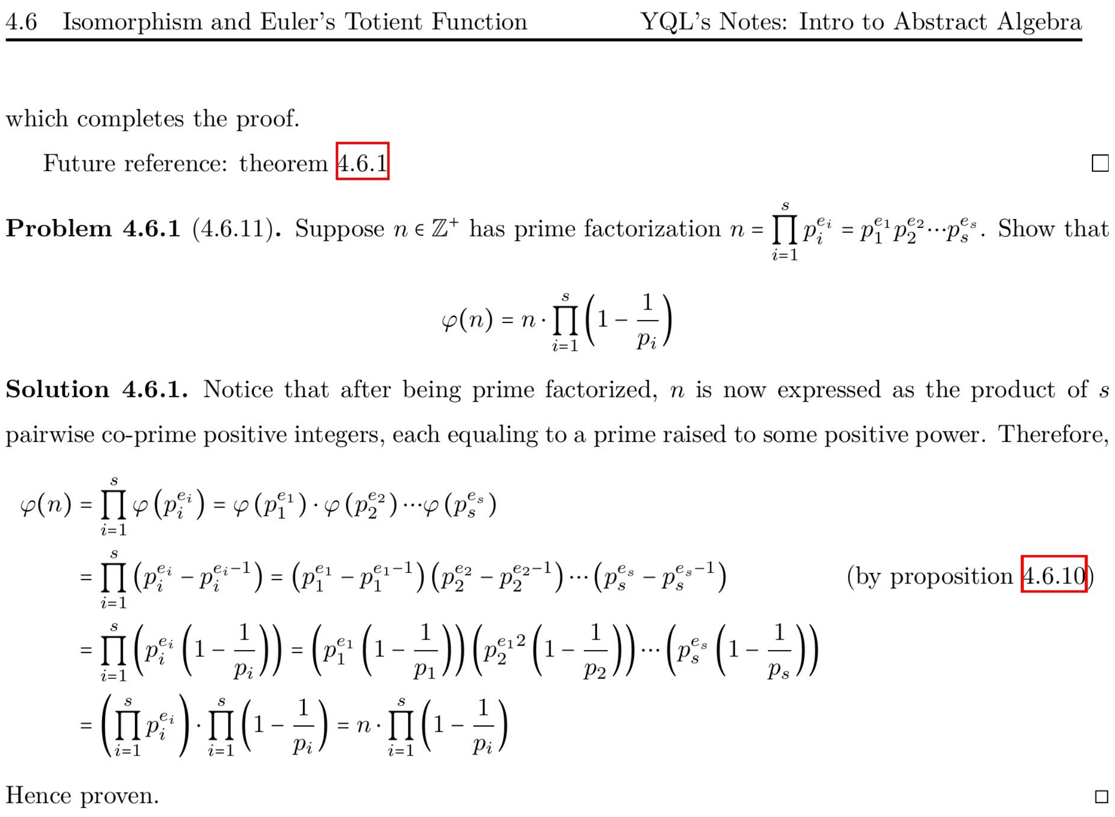
(2) Likewise, for $(\mathbb{Z}/229\mathbb{Z})^*$, we know it is isomorphic to $(\mathbb{Z}/228\mathbb{Z}, +)$, and the number of generators is $\varphi(228) = 228 \cdot (1/2) \cdot (2/3) \cdot (18/19) = 72^\dagger$.

Remark

In general, $(\mathbb{Z}/m\mathbb{Z})^*$ has $\varphi(m-1)$ generators.

Remark: on Euler's Totient Function

I computed $\varphi(28)$ and $\varphi(228)$ using the following proposition. The screenshot is taken from one of my previous notes.



4.6 Isomorphism and Euler's Totient Function YQL's Notes: Intro to Abstract Algebra

which completes the proof.

Future reference: theorem 4.6.1 □

Problem 4.6.1 (4.6.11)**.** Suppose $n \in \mathbb{Z}^+$ has prime factorization $n = \prod_{i=1}^{s} p_i^{e_i} = p_1^{e_1} p_2^{e_2} \cdots p_s^{e_s}$. Show that

$$\varphi(n) = n \cdot \prod_{i=1}^{s} \left(1 - \frac{1}{p_i}\right)$$

Solution 4.6.1. Notice that after being prime factorized, n is now expressed as the product of s pairwise co-prime positive integers, each equaling to a prime raised to some positive power. Therefore,

$$\begin{aligned}
\varphi(n) &= \prod_{i=1}^{s} \varphi\left(p_i^{e_i}\right) = \varphi\left(p_1^{e_1}\right) \cdot \varphi\left(p_2^{e_2}\right) \cdots \varphi\left(p_s^{e_s}\right) \\
&= \prod_{i=1}^{s} \left(p_i^{e_i} - p_i^{e_i - 1}\right) = \left(p_1^{e_1} - p_1^{e_1 - 1}\right)\left(p_2^{e_2} - p_2^{e_2 - 1}\right) \cdots \left(p_s^{e_s} - p_s^{e_s - 1}\right) && \text{(by proposition 4.6.10)} \\
&= \prod_{i=1}^{s} \left(p_i^{e_i}\left(1 - \frac{1}{p_i}\right)\right) = \left(p_1^{e_1}\left(1 - \frac{1}{p_1}\right)\right)\left(p_2^{e_1 2}\left(1 - \frac{1}{p_2}\right)\right) \cdots \left(p_s^{e_s}\left(1 - \frac{1}{p_s}\right)\right) \\
&= \left(\prod_{i=1}^{s} p_i^{e_i}\right) \cdot \prod_{i=1}^{s} \left(1 - \frac{1}{p_i}\right) = n \cdot \prod_{i=1}^{s} \left(1 - \frac{1}{p_i}\right)
\end{aligned}$$

Hence proven. □