The third problem set: due 10/30/14.

Wednesday, October 22, 2014
10:22 AM

1. Let a and b be two positive integers. Prove that

$$\frac{a}{\gcd(a,b)} \quad \text{and} \quad \frac{b}{\gcd(a,b)}$$ are relatively prime.

2. Let $SL_2(\mathbb{Z}) := \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \;\middle|\; \begin{array}{l} a,b,c,d \in \mathbb{Z} \\ \text{and } ad-bc=1 \end{array} \right\}$.

(i) Prove that, if $x \in SL_2(\mathbb{Z})$, then $\exists y \in SL_2(\mathbb{Z})$

s.t. $xy = yx = I$ where $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$.

(ii) Prove that, if $x_1, x_2 \in SL_2(\mathbb{Z})$, then

$$x_1 x_2 \in SL_2(\mathbb{Z})$$

(Remark. You are proving that $SL_2(\mathbb{Z})$ is a subgroup of $GL_2(\mathbb{R})$.)

3. Let $SL_2(\mathbb{Z})$ be as in problem 2. Prove that

$$\left\{ x \begin{bmatrix} 1 \\ 0 \end{bmatrix} \;\middle|\; x \in SL_2(\mathbb{Z}) \right\} = \left\{ \begin{bmatrix} a \\ b \end{bmatrix} \;\middle|\; \begin{array}{l} a,b \in \mathbb{Z} \\ \gcd(a,b)=1 \end{array} \right\}$$

4. Let $n \in \mathbb{Z}^{>1}$ and $a \in \mathbb{Z}$. Suppose

$$a^d \equiv 1 \pmod{n} \quad \text{and} \quad a^2 \not\equiv 1 \pmod{n}$$

for $1 \le i < d$.

Prove that $a^m \equiv 1 \pmod n \iff d \mid m$.

(Remark. d is called the multiplicative order of a modulo n. In some books, it is denoted by $\mathrm{Ord}_n(a)$.)

5.(i) Use problem 4 to prove the following:

$$\left.\begin{array}{l} a^m \equiv 1 \pmod d \\ a^n \equiv 1 \pmod d \end{array}\right\} \Rightarrow a^{\gcd(m,n)} \equiv 1 \pmod d$$

(ii) Use problem 4 to prove that

$$k \mid m \Rightarrow a^k - 1 \mid a^m - 1.$$

(iii) Use parts (i) and (ii) to prove

$$\gcd(a^n - 1, a^m - 1) = a^{\gcd(m,n)} - 1.$$

(Hint: For part (ii) notice that $a^k \equiv 1 \pmod{a^k - 1}$.)

6. Let $\mathbb{Z}_n^\times := \{[a]_n \in \mathbb{Z}_n \mid \exists a' \in \mathbb{Z} \text{ s.t. } [a]_n [a']_n = [1]_n\}$.

Prove that $(\mathbb{Z}_n^\times, \cdot)$ is a group.

In class we proved that the function

$$\mathbb{Z}_{mn} \xrightarrow{f} \mathbb{Z}_m \times \mathbb{Z}_n$$

$$[a]_{mn} \longmapsto ([a]_m, [a]_n)$$

is a bijection if $\gcd(m,n)=1$.

7. (i) Prove that for any $x, y \in \mathbb{Z}_{mn}$ we have

$$f(x+y) = f(x) + f(y)$$

and $$f(x \cdot y) = f(x) \cdot f(y)$$

(In $\mathbb{Z}_m \times \mathbb{Z}_n$, we add and multiply componentwise.)

(ii) Let $\mathbb{Z}_{mn}^{\times}$ be as in Problem 6, and

$$(\mathbb{Z}_m \times \mathbb{Z}_n)^{\times} := \{ (a,b) \mid \exists (a',b') \in \mathbb{Z}_m \times \mathbb{Z}_n \text{ s.t. } (a,b)\cdot(a',b') = ([1]_m, [1]_n) \}.$$

Prove that f induces a bijection between

$\mathbb{Z}_{mn}^{\times}$ and $(\mathbb{Z}_m \times \mathbb{Z}_n)^{\times}$.

(We already know f is 1-1; You have to

show ⓐ if $x \in \mathbb{Z}_{mn}^{\times}$, then $f(x) \in (\mathbb{Z}_m \times \mathbb{Z}_n)^{\times}$.

ⓑ if $f(x) \in (\mathbb{Z}_m \times \mathbb{Z}_n)^\times$, then $x \in \mathbb{Z}_{mn}^\times$.

For the second part notice that

$$f([1]_{mn}) = ([1]_m, [1]_n)$$

and f is 1-1.)

8. Let m and n be two relatively prime integers.

And $(\mathbb{Z}_m \times \mathbb{Z}_n)^\times$ be as in Problem 7.

(i) Prove that $(\mathbb{Z}_m \times \mathbb{Z}_n)^\times = \mathbb{Z}_m^\times \times \mathbb{Z}_n^\times$.

(ii) Use Problem 7 and part (i) to conclude

$$|\mathbb{Z}_{mn}^\times| = |\mathbb{Z}_m^\times||\mathbb{Z}_n^\times|.$$

(iii) Prove that $|\mathbb{Z}_{p^k}^\times| = p^{k-1}(p-1)$ if p is prime

(iv) Use parts (ii) and (iii) to prove

$$|\mathbb{Z}_{p_1^{k_1} \cdots p_m^{k_m}}^\times| = \prod_{i=1}^{m} p_i^{k_i - 1}(p_i - 1)$$

where $p_1 < \cdots < p_m$ are primes and

$k_1, \ldots, k_m \in \mathbb{Z}^+$.