The forth problem set: due 11/05/14

Wednesday, October 29, 2014
10:15 AM

1. Find all the solutions of

$$[14]_{21}[x]_{21} = [28]_{21}.$$

2. Find all the solutions of

$$x \overset{8}{\equiv} 5$$
$$x \overset{9}{\equiv} 7.$$

3. Let $(G, \cdot)$ be a group. Let e be the identity element of G. Suppose for any $a \in G$ we have

$$a^2 = e.$$

Prove that G is abelian, i.e. $ab = ba$ for any $a, b \in G$.

4. Let $n \in \mathbb{Z}^{\geq 2}$. Prove that for any $[a]_n$

either $\exists [b]_n$ s.t. $[a]_n [b]_n = [1]_n$

or $\exists [b]_n$ s.t. $[a]_n [b]_n = [0]_n$.

(Any element is either a unit or a zero-divisor.)

5. Let p be a prime number. Then we know

$$\mathbb{Z}_p^\times = \mathbb{Z}_p \setminus \{0\}.$$

(i) Prove that $[a]_p = [a]_p^{-1} \Longleftrightarrow [a]_p = [\pm 1]_p$.

(ii) Prove that $[1]_p \cdot [2]_p \cdot \dots \cdot [p-1]_p = [-1]_p$

(This is equivalent to $(p-1)! \equiv -1 \pmod{p}$.

Hint for (ii) Pair each term with its modular inverse and notice that by part (i) you can actually do it unless the term is either $[1]_p$ or $[p-1]_p$.)

6. Let $n \in \mathbb{Z}^{\geq 1}$. For a divisor d of n, let

$$A_d := \{ k \in \mathbb{Z} \mid 1 \leq k \leq n, \ \gcd(k,n) = d \}.$$

(i) Prove that $|A_d| = \varphi(\frac{n}{d})$.

[Recall. $\varphi(m) = |\mathbb{Z}_m^\times| = \left| \{ \ell \in \mathbb{Z} \mid 1 \leq \ell \leq m, \ \gcd(\ell, m) = 1 \} \right|$.

Hint. $\gcd(k,n) = d \Longleftrightarrow \gcd(\frac{k}{d}, \frac{n}{d}) = 1$.]

(ii) Prove that $\sum_{d \mid n} \varphi(n/d) = n$.

[Hint. Notice that $\{1,2,\cdots,n\} = \bigcup_{d|n} A_d$

and $A_{d_1} \cap A_{d_2} = \emptyset$ if $d_1 \neq d_2$.]

7. Let p be a prime number. Prove that, for any $a, b \in \mathbb{Z}$, we have

$$([a]_p + [b]_p)^p = [a]_p^p + [b]_p^p .$$

(Hint. One approach is to use the binomial expansion:

$$(x+y)^n = \sum_{i=0}^{n} \binom{n}{i} x^i y^{n-i}$$

where $\binom{n}{i} = \frac{n!}{i!\,(n-i)!} = \frac{n(n-1)\cdots(n-i+1)}{i!}$. And then show $p \mid \binom{p}{i}$ if p is prime and $1 \le i \le p-1$.)