Math 471 Midterm 2 Spring 2019

Name: Solution

1. (20 points) Let $n = pq$ with p and q distinct primes and let a be a natural number satisfying $\gcd(n, a) = 1$. Prove the equality $\bar{a}^{n+1} = \bar{a}^{p+q}$ in $\mathbb{Z}_n$. Hint: Use Euler's Theorem. (6 pt)

The Euler number of n is $\varphi(n) = \varphi(p)\,\varphi(q) = (p-1)(q-1)$

The equality $\gcd(n,a) = 1$ is the hypothesis in Euler's Theorem, which states that $\bar{a}^{\varphi(n)} = \bar{1}$ in $\mathbb{Z}_n$. (6 pt)

Hence,

$$\bar{1} = \bar{a}^{(p-1)(q-1)} = \bar{a}^{pq+1-p-q} = \bar{a}^{n+1-p-q}.$$

Mutiply both sides by $\bar{a}^{(p+q)}$ to get (3 pt)

$$\bar{a}^{p+q} = \bar{a}^{n+1}.$$

Q. E. D.

15 pts

2. (27 points) a) Let a, b, c be integers and n a natural number. Set $d := \gcd(c, n)$. Prove that $ca \equiv cb \pmod{n}$, if and only if $a \equiv b \pmod{n/d}$. Hint: Write $n = dn_1$, $c = dc_1$ and observe that n_1 and c_1 are relatively prime. Then Start with the definition of $x \equiv y \pmod{n}$ in one direction and with that of $x \equiv y \pmod{n/d}$ in the other direction.

Set $d := \gcd(c, n)$ and write $n = dn_1$, $c = dc_1$.

Then $\gcd(n_1, c_1) = \gcd\left(\frac{n}{d}, \frac{c}{d}\right) = \frac{\gcd(n, c)}{d} = \frac{d}{d} = 1$,

(↑ A Theorem)

Assume $ca \equiv cb \pmod{n}$. Then $n \mid \underbrace{ca - cb}_{c(a-b)}$.

So $dn_1 \mid dc_1(a-b)$.

So $n_1 \mid c_1(a-b)$. Now $\gcd(n_1, c_1) = 1$, and so

$n_1 \mid (a-b)$, by Euclid's Lemma.

So $a \equiv b \pmod{n_1 = \frac{n}{d}}$.

Conversely, assume $a \equiv b \pmod{\frac{n}{d} = n_1}$. Then $n_1 \mid a-b$.

So $\underbrace{dn_1}_{n} \mid d(a-b)$. So $n \mid d(a-b)$. So

$n \mid \underbrace{dc_1}_{c}(a-b)$. So $n \mid ca - cb$, So $ca \equiv cb \pmod{n}$.

12 pts

b) How many elements of $\mathbb{Z}_{174}$ are the reduction of $34a$, for some integer a? Justify your answer. Hint: Use part a).

Let a, b be integers. Then

$34a \equiv 34b \pmod{174}$ if and only if

$a \equiv b \pmod{\frac{174}{\gcd(34, 174)}}$, by part a.

$\gcd(34, 174)$: $34 = 2 \cdot 17$, $174 = 2 \cdot 3 \cdot 29$, so $\gcd = 2$

$\frac{174}{2} = 87$

So, $34a \equiv 34b \pmod{174} \iff a \equiv b \pmod{87}$.

So $\overline{34}\,\bar{a} = \overline{34}\,\bar{b}$ in $\mathbb{Z}_{174} \iff \bar{a} \equiv \bar{b} \pmod{87}$

Hence, the 87 classes

$\overline{34 \cdot 0}, \overline{34 \cdot 1}, \overline{34 \cdot 2}, \ldots, \overline{34 \cdot 86}$ are distinct classes in $\mathbb{Z}_{174}$, and they include all classes of the form $\overline{34 \cdot a}$, with $a \in \mathbb{Z}$, since there exists $0 \leq r \leq 86$, such that $\bar{a} = \bar{r} \pmod{87}$.

We conclud that there are 87 such classes.

8 pt

3. (30 points) a) Show that the order of any non-zero element of $\mathbb{Z}_{29}$ must be one of 1, 2, 4, 7, 14, or 28.

$p=29$ is a prime. Hence, $\bar{a} \neq \bar{0} \Rightarrow \bar{a}^{28} = \bar{1}$ in $\mathbb{Z}_{29}$, by Fermat's Little Thm. Hence $\text{ord}(\bar{a}) \mid 28$, if $\bar{a} \neq 0$.
$28 = 2^2 \cdot 7$. So the set of divisors of 28 is

$$\{2^k \cdot 7^j : 0 \leq k \leq 2,\ 0 \leq j \leq 1\} = \{1, 2, 4, 7, 14, 28\}.$$

8 pt

b) Use part a) to show that $\bar{2}$ is a primitive root in $\mathbb{Z}_{29}$.

We need to show that $\text{ord}(\bar{2}) = 28$.
It suffices to show that $\bar{2}^{14}$ and $\bar{2}^{4}$ are non-zero, since every divisor of 28 other than 28 divides one of 4 or 14,

$\bar{2}^4 = \overline{16} \neq \bar{1}$ in $\mathbb{Z}_{29}$.

$\bar{2}^8 = \overline{256} = \overline{24} = -\bar{5}$ in $\mathbb{Z}_{29}$

$\bar{2}^{14} = \bar{2}^8 \cdot \bar{2}^4 \cdot \bar{2}^2 = -\bar{5} \cdot \underbrace{\overline{16} \cdot \overline{4}}_{\overline{64} = \overline{6}} = -\overline{30} = -\bar{1} = \overline{28} \neq \bar{1}$

7 pts

c) For each of the six values listed in part a), find an element of $\mathbb{Z}_{29}$ of that order. Prove that the order is as you state it to be.

If $d \mid 28$, $cd = 28$, then

$$\operatorname{ord}(\bar{2}^c) = \frac{\operatorname{ord}(\bar{2})}{c} = \frac{28}{c} = d.$$

Thus, $\operatorname{ord}(\bar{1}) = 1$, $\operatorname{ord}(-\bar{1}) = 2$, $\operatorname{ord}(\bar{2}^7) = 4$,
$\operatorname{ord}(\bar{2}^4) = 7$, $\operatorname{ord}(\bar{2}^2) = 14$, $\operatorname{ord}(\bar{2}) = 28$

7 pts

d) How many primitive roots are there in $\mathbb{Z}_{29}$?

(*) $\bar{2}^c$ is primitive $\Leftrightarrow \dfrac{\operatorname{ord}(\bar{2})}{\gcd(c, \operatorname{ord}(\bar{2}))} = 28 \Leftrightarrow \dfrac{28}{\gcd(c, 28)} = 28$

$\Leftrightarrow \gcd(c, 28) = 1.$

All powers $\bar{2}^c$ are obtained, without repetition, as c ranges from 1 to 28, and precisely $\boxed{\varphi(28)}$ of them are primitive, by (*).

$$\varphi(28) = \underbrace{\varphi(2^2)}_{2^2-2=2} \cdot \underbrace{\varphi(7)}_{6} = \boxed{12}$$

4. (27 points) Consider the RSA encryption scheme with $n = 391 = 17 \cdot 23$. a) Is $e = 121$ a valid encryption exponent? Justify your answer.

$121 = 11^2$

$\varphi(n) = (17-1)(23-1) = 16 \cdot 22 = 2^5 \cdot 11$

$\gcd(\varphi(n), e) = \gcd(2^5 \cdot 11, 11^2) = 11 \neq 1,$

so e is not a valid encryption exponent.

b) For the encryption exponent $e = 5$, find the decryption exponent. d

$\varphi(n) = 16 \cdot 22 = 352$

We need $de \equiv 1 \pmod{\varphi(n)}$. Solve the Diophantine eq $352x + 5d = 1$

x_i	d_i	r_i	q_i
1	0	352	
0	1	5	
1	-70	2	70
-2	141	1	2

$352(-2) + 5(141) = 1.$

So $d = 141$ is the decryption exponent.

c) Encrypt the message 13. $e = 5 = 4+1$

$13^2 = 169$

$13^4 = 169^2 \equiv 18 \pmod{391}$

$13^5 = 18 \cdot 13 \equiv 234 \pmod{391}$