Number Theory 2023 Final Solutions

(This has solutions to questions from both classes tests. Some questions were the same but with different numbers. I've only put the solution for one version.)

1. Demonstrate the method of successive squaring as you compute $46^{57} \bmod 13$.

Solution

$46^{57} \equiv_{13} 7^{57} \equiv 7^9 = 7^8 \cdot 7$. By succssive squaring we compute

$7^2 \equiv_{13} 10 \equiv_{13} -3 \qquad 7^4 \equiv_{13} (-3)^2 = 9 \equiv_{13} -4 \qquad 7^8 \equiv (-4)^2 \equiv 3$

and so get $46^{57} \equiv_{13} 7(3) \equiv_{13} \boxed{8}$.

2. Decode the message $c = 4$ to the original message m that was encoded with RSA modulus $n = 55$ and exponent $e = 23$.

Solution

We use the EEA to get the decoding exponent $d = 23^{-1}$ modulo $\phi(55) = 40$.

			40	23
40	$= (1)23+$	17	1	-1
23	$= (1)17+$	6	-1	$1+1$
17	$= (3)6+$	-1	$1+3$	$-1-6$

So $(7)23 - (4)40 = 1$ and so $23^{-1} \equiv_{40} 7$.

So $m = \boxed{4^7 \mod 55} = 4{\cdot}4^2{\cdot}4^4 \equiv 4{\cdot}16{\cdot}{-19} \equiv -21{\cdot}16 \equiv -29{\cdot}4 \equiv -6 \equiv \boxed{49}$.

3. Where $n = 1105$, we find that $n-1 = 1104 = 2^4 \cdot 69$. We compute, the following modulo 1105. Fill in the chart with Y or N signifying which values of a are Euler witnesses and which are Miller Rabin witnesses (witnessing the fact that n is composite)?

a	a^{69}	$a^{2\cdot 69}$	$a^{2^2\cdot 69}$	$a^{2^3\cdot 69}$	$a^{2^4\cdot 69}$	Euler witness?	MR witness?
15	70	480	560	885	885		
47	47	-1	1	1	1		
66	716	1048	781	1	1		
81	846	781	1	1	1		

Solution

a	a^{69}	$a^{2\cdot 69}$	$a^{2^2\cdot 69}$	$a^{2^3\cdot 69}$	$a^{2^4\cdot 69}$	Euler witness?	MR witness?
15	70	480	560	885	885	Y	Y
47	47	-1	1	1	1	N	N
66	716	1048	781	1	1	N	Y
81	846	781	1	1	1	N	Y

4. Which of the following are Carmichael numbers? For those that are not, give a reason.

   (a) 1105 (Note: $1105 = 5 \cdot 13 \cdot 17$ and $1104 = 2^4 \cdot 3 \cdot 23$.)

   (b) 1235 (Note: $1235 = 5 \cdot 13 \cdot 19$ and $1234 = 2 \cdot 617$.)

   (c) 19747 (Note: $19747 = 7^2 \cdot 13 \cdot 31$ and $19746 = 2 \cdot 3^2 \cdot 1097$)

Solution

Using Korselt's criterium 1105 is, 1235 isn't as $(5-1) \nmid (1235-1)$, and 19747 isn't as it is not the product of distinct primes.

5. Let $p \geq 5$ be a prime. Let Q be the set of elements in $\{1, \ldots, p-1\}$ that are QR modulo p.

   (a) Show that $\sum_{a \in Q} a \equiv_p 0$.

   (b) Show that if $p \equiv_4 1$ then $\sum_{a \in Q} a = p(p-1)/4$.

Solution

(a) Let c be an NR mod p other than -1 (this is why we need $p \geq 5$). For any QR n the number cn mod p is an NR, and as c is invertible, every NR is cn for some QR n. So $\sum NR \equiv_p \sum c \cdot QR \equiv_p c \sum QR$, which means $(1+c)\sum QR = \sum QR + \sum NR = p(p-1)/2 \equiv_p 0$ As c is not $p-1$, $c+1$ is invertible mod p, so dividing both sides of this last equation by $c+1$, we get $\sum QR \equiv_p 0$.

(b) If $p \equiv_4 1$ then -1 is a QR, so n is a QR if and only if $p-n$ is. It follows that the $(p-1)/2$ QR pair up into $(p-1)/4$ pairs that sum to p. Thus $\sum QR = p(p-1)/4$.

6. (a) Fill in the following: for any _____ a and b we have

$$\left(\frac{-1}{b}\right) = \begin{cases} 1 & \text{if } \_\_\_\_\_ \\ -1 & \text{if } \_\_\_\_\_ \end{cases}$$

$$\left(\frac{2}{b}\right) = \begin{cases} 1 & \text{if } \_\_\_\_\_ \\ -1 & \text{if } \_\_\_\_\_ \end{cases}$$

$$\left(\frac{a}{b}\right) = \begin{cases} \left(\frac{b}{a}\right) & \text{if } \_\_\_\_\_ \\ -\left(\frac{b}{a}\right) & \text{if } \_\_\_\_\_ \end{cases}$$

(b) Deterimine if 37 is a QR modulo the prime 101

Solution

(a) For any distinct odd integers a and b we have

- $\left(\frac{-1}{b}\right) = \begin{cases} 1 & \text{if } b \equiv_4 1 \\ -1 & \text{if } b \equiv_4 3 \end{cases}$
- $\left(\frac{2}{b}\right) = \begin{cases} 1 & \text{if } b \equiv_8 1, 7 \\ -1 & \text{if } b \equiv_8 3, 5 \end{cases}$
- $\left(\frac{a}{b}\right) = \begin{cases} \left(\frac{b}{a}\right) & \text{if } b \equiv_4 1 \text{ or } a \equiv_4 1 \\ -\left(\frac{b}{a}\right) & \text{if } a \equiv_4 b \equiv_4 3 \end{cases}$

(b) Computing the Legendre symbol $\left(\frac{47}{101}\right)$ we get

$$\left(\frac{47}{101}\right) = \left(\frac{101}{47}\right) = \left(\frac{7}{47}\right) = -\left(\frac{47}{7}\right) = -\left(\frac{5}{7}\right) = -\left(\frac{7}{5}\right) = -\left(\frac{2}{5}\right) = 1$$

so $\boxed{47 \text{ is a quadratic residue modulo } 101}$.

7. **By computing Legendre Symbols,** determine if 35 and 141 are QR modulo the prime $p = 101$.

Solution

Sorry! I forgot to put $p = 101$ in this question. I only had p. This made it fairly confusing, so I didn't use the question.

$$\left(\frac{35}{101}\right) = \left(\frac{7}{101}\right)\left(\frac{5}{101}\right) = \left(\frac{101}{7}\right)\left(\frac{101}{5}\right) = \left(\frac{3}{7}\right)\left(\frac{1}{7}\right) = -\left(\frac{7}{3}\right) = -\left(\frac{1}{3}\right) = -1$$

so 35 is not a QR, and

$$\left(\frac{141}{101}\right) = \left(\frac{40}{101}\right) = \left(\frac{2}{101}\right)\left(\frac{5}{101}\right) = (-1)\left(\frac{101}{5}\right) = -\left(\frac{1}{5}\right) = -1$$

so 141 is not either.

8. Show that there are infinitely many primes congruent to 1 modulo 3.

Solution

Assume, towards contradiction, that there are finitely many: $p_1, \ldots, p_n$. Where $A = (2\Sigma_{i=1}^{n} p_i)^2 + 3$, we have $A \equiv_3 2^2 + 3 \equiv_3 1$, and so A cannot be prime. But also none of 2 or the p_i divide A, so all primes q_j dividing A have $q_j \equiv_3 2$. Moreover $A \equiv_4 3$ so some q dividing A also has $q \equiv_4 3$. It follows then, that $2\Sigma p_i$ is a solution to $x^2 \equiv_q -3$, telling us that -3 is a QR modulo q. But as $q \equiv_4 1$ we have $\left(\frac{-3}{q}\right) = \left(\frac{-1}{q}\right)\left(\frac{3}{q}\right) = \left(\frac{3}{q}\right) = \left(\frac{q}{3}\right) = \left(\frac{2}{3}\right) = -1$, so this is a contradiction.

9. Observe that $26^2 + 15^2 = 17 \cdot 53$. **Using the method of descent**, write a smaller multiple of 53 as a sum of two squares.

Solution

Where $A = 26$ and $B = 15$ we reduce them symmetrically modulo 17 to get $a = -8$ and $b = -2$, giving us

$$64 + 4 = a^2 + b^2 = 4 \cdot 17.$$

Using the equation $(A^2 + B^2)(a^2 + b^2) = (aA + bB)^2 + (bA - aB)^2$ we get

$$(-8 \cdot 26 - 2 \cdot 15)^2 + (2 \cdot 26 - 8 \cdot 15)^2 = 4 \cdot 17^2 \cdot 53$$

dividing through by 17^2 we get

$$14^2 + 4^2 = 4 \cdot 53.$$

10. Find positive integers A, B and M such that $A^2 + B^2 = M \cdot 1105$. (The table from Question 3 might help).

Solution

From the table on Questions 3 we see that $47^2 \equiv_{1105} -1$ and so $1105 | 47^2 + 1^2$. As $47^2 \approx 2200$ we clearly have $\boxed{47^2 + 1^2 = 2 \cdot 1105}$.

11. Write $1189 = 29 \cdot 41$ as a sum of squares (you can skip descent if you can see the answer), and then use this to find a primitive pythagorean triple $(a, b, 1189)$.

Solution

We have that $29 = 5^2 + 2^2$ and $41 = 5^2 + 4^2$ so $1189 = (5 \cdot 5 + 2 \cdot 4)^2 + (2 \cdot 5 - 5 \cdot 4)^2 = 33^2 + 10^2$. That is $\boxed{1189 = 33^2 + 10^2}$. (Or $1189 = (5 \cdot 4 + 2 \cdot 5)^2 + (5 \cdot 5 - 2 \cdot 4)^2 = 30^2 + 13^2$.)

So

$2(1189) = (1^2+1^2)(33^2+10^2) = (33 \cdot 1+10 \cdot 1)^2+(33 \cdot 1-10 \cdot 1)^2 = 43^2+23^2 =: s^2+t^2$.

And so we have the PPT

$$(st, \frac{s^2 - t^2}{2}, \frac{s^2 + t^2}{2}) = \boxed{(43 \cdot 23, \frac{43^2 - 23^2}{2}, 1189)} = (989, 660, 1189).$$

12. Let $\lambda(1) = 1$ and where n has prime decomposition $n = \prod_{i=1}^{t} p_i^{k_i}$ let $\lambda(n) = (-1)^{k_1+\cdots+k_t}$. Let $G(n) = \sum_{d|n} \lambda(d)$.

    (a) Show that $G(p) = 0$ for prime p.

    (b) What is $G(p^d)$ for prime p.

    (c) Find a formula for $G(n)$.

    (d) Compute $\lambda(30800)$ and $G(30800)$.

Solution

(a) We have $G(p) = \lambda(1) + \lambda(p) = 1 - 1 = 0$, and

(b) $G(p^d) = \sum_{i=1}^{d} \lambda(p^i)$ is 0 if d is odd, and is 1 if d is even; so it is $\boxed{G(p^d) = d + 1 \mod 2}$.

(c) As λ is multiplicative by definition, $G(n)$ is multiplicative, and so for $n > 1$, $G(n) = \prod_{i=1}^{t} G(p_i^{k_i})$ is 1 if and only if all of the k_i are even. That is $\boxed{G(n) \text{ is 1 if } n \text{ is a square, and is 0 otherwise}}$.

(d) As $30800 = 2^4 \cdot 5^2 \cdot 7 \cdot 11$ we have that $\lambda(30800) = 1 \cdot 1 \cdot -1 \cdot -1 = \boxed{1}$ and $\boxed{G(n) = 0}$.

13. Using the index table below, solve the congruences

    (a) $23x \equiv_{31} 26$

    (b) $2x^{13} \equiv_{31} 18$

Solution

Generator $g = 3$. Part i) the index equation is

$$I(x) \equiv_{30} I(26) - I(23) = 5 - 27 = -22 \equiv_{30} 8.$$

So $\boxed{x = 20}$.

Part ii) the index equation is

$$\begin{aligned} & 13I(x) \equiv_{30} I(18) - I(2) \\ \iff \quad & 13I(x) \equiv_{30} 26 - 24 \qquad = 2. \end{aligned}$$

As $\gcd(13, 30) = 1$ this has a solution. Generally we would find the inverse of 13 mod 30 by the Extended Euclidean algorithm, but we all know that $7 \cdot 13 = 91 \equiv_{30} 1$. So $13^{-1} \equiv_{30} 7$. Using this, $I(x) \equiv_{30} 2 \cdot 7 = 14$, and so $\boxed{x = 10}$.

Modulo $p = 31$ for generator $g = 3$.

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
3^a	3	9	27	19	26	16	17	20	29	25	13	8	24	10	30
a	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
3^a	28	22	4	12	5	15	14	11	2	6	18	23	7	21	1

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$I(a)$	30	24	1	18	20	25	28	12	2	14	23	19	11	22	21
a	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
$I(a)$	6	7	26	4	8	29	17	27	13	10	5	3	16	9	15