Number Theory 2018 Final Solutions

1. Solve the congruence $x^{113} \equiv_{47} 363$.

Solution

Reducing 363 modulo 47 and using Fermat's Little Theorem to reduce 113 modulo $\phi(47) = 46$, the equation becomes $x^{21} \equiv_{47} 34$. Using the EEA we find the inverse of 19 modulo 46:

A	$=$	B	$\cdot$	Q	$+$	R	46	21
46	$=$	21	$\cdot$	2	$+$	4	1	-2
21	$=$	4	$\cdot$	5	$+$	1	$-5(1) = -5$	$1 - 5(-2) = \boxed{11}$

So $21^{-1} \equiv_{46} 11$. Now by successive squaring we compute 34^{11}. As $11 = 2^3 + 2^1 + 2^0$ we compute first

i	34^{2^i} mod 463
0	34
1	38
2	32
3	37

And then get $34^{11} \equiv_{47} 37 * 28 * 34 \equiv 21$. So $\boxed{x = 21}$.

2. Let $m = pq$ for distinct primes p and q. Show for **any** number $a \in \{1, 2, \ldots, m-1\}$ that $a^{\phi(m)+1} \equiv_m a$.

Solution

It is not enough to use just Fermat's little theorem, this only shows it when $\gcd(a, m) = 1$!

Here's how we do it.
Using Fermat's little theorem, observe that

$$a^{\phi(m)+1} = a^{\phi(q)\phi(p)+1} = (a^{\phi(q)})^{\phi(p)} \cdot a \equiv_q a$$

so $q \mid (a^{\phi(m)+1} - a)$. Similarly we get $p \mid (a^{\phi(m)+1} - a)$. As p and q are relatively prime, this gives us $m = pq \mid (a^{\phi(m)+1} - a)$, and so $a^{\phi(m)+1} \equiv_m a$.

3. Which of the following are definitely composite? (And which are likely prime considering the given Miller-Rabin test?)

   (a) 19277. Note that $19277 - 1 = 2^2 \cdot 4819$, and that

i	$2^{4819 \cdot 2^i}$ mod 19277
0	15118
1	5212
2	6040

(b) 19289. Note that $19289 - 1 = 2^3 \cdot 2411$ and that

i	$3^{2411 \cdot 2^i}$ mod 19289
0	3511
1	1450
2	19288
3	1

(c) 19301. Note that $19301 - 1 = 2^2 \cdot 4825$ and that

i	$5^{4825 \cdot 2^i}$ mod 19301
0	1

Solution

19277 is composite, the other two are likely prime. Notice, in (b), that $19288 \equiv_{19289} -1$. (Sorry. It was a mean joke.)

4. (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) Determine if 37 is a quadratic residue modulo the prime 43.

Solution

(a) For any distinct positive 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 $\left(\frac{37}{43}\right)$ we get

$$\left(\frac{37}{43}\right) = \left(\frac{43}{37}\right) = \left(\frac{6}{37}\right) = \left(\frac{2}{37}\right)\left(\frac{3}{37}\right) = -\left(\frac{3}{37}\right) = -\left(\frac{37}{3}\right) = -\left(\frac{1}{3}\right) = -1$$

so $\boxed{37 \text{ is not a quadratic residue modulo } 43}$.

5. Assuming that it holds when b is prime, prove your statement
$\left(\frac{2}{b}\right) = \begin{cases} 1 & \text{if} \\ -1 & \text{if} \end{cases}$
from question (4), for any positive odd integer b.

Solution

For an odd prime b we have a prime decomposition

$$b = p_1 \cdots p_s \cdot q_1 \cdots q_t$$

where for each i, $p_i \equiv_8 \pm 1$ and for each j, $q_j \equiv_8 4 \pm 1$.
Noticing that $\pm 1 \cdot \pm 1 = \pm 1$, that $(4 \pm 1) \cdot (4 \pm 1) \equiv_8 \pm 1$ and that $\pm 1 \cdot (4 \pm 1) \equiv_8 (4 \pm 1)$ we get that $b \equiv_8 4 \pm 1$ if and only if t is odd.
Computing the Legendre symbol, we get

$$\left(\frac{2}{b}\right) = \prod_{i=1}^{s} \left(\frac{2}{p_i}\right) \prod_{j=1}^{t} \left(\frac{2}{q_j}\right) = (1)^s(-1)^t.$$

which is -1 if and only if t is odd, correponding exactly with the case that $b \equiv_8 4 \pm 1$, as needed.

6. Which of the following numbers can be written as the sum of two squares: 137, 145, 175, 490?

Solution

$137 \equiv_4 1$ is a prime so $\boxed{137 \text{ can}}$ be written as a product of two squares.
$145 = 5 \cdot 29$ both factors are $\equiv_4 1$ so $\boxed{145 \text{ can}}$ too.
$175 = 5^2 \cdot 7$ but $7 \equiv_4 3$, so $\boxed{175 \text{ can't}}$.
$490 = 2 \cdot 5 \cdot (7)^2$, so $\boxed{490 \text{ can}}$.

7. Observe that $23^2 + 115^2 = 13 \cdot 1058$. Write a smaller multiple of 1058 as a sum of two squares.

Solution

Let $A = 23 \equiv_{13} 10 \equiv_{13} -3$ and $B = 115 \equiv_{13} 11 \equiv_{13} -2$. So we have both

$$23^2 + 115^2 = 13 \cdot 1058 \text{ and } 3^2 + 2^2 = 13 \cdot 1.$$

Using the equation $(u^2 + v^2)(A^2 + B^2) = (uA + vB)^2 + (vA - uB)^2$ we get

$$13^2 \cdot (1058) = (23 * 3 + 115 * 2)^2 + (23 * 2 - 115 * 3)^2$$

dividing through by 13^2 we get

$$1058 = \left(\frac{23 * 3 + 115 * 2}{13}\right)^2 + \left(\frac{23 * 2 - 115 * 3}{13}\right)^2 = 23^3 + 23^2.$$

8. (a) Define *primitive root modulo p*.

   (b) How many primitive roots are there modulo 47?

   (c) Find a primitive root modulo 13.

   (d) Show that if a is a primitive root modulo p and $\gcd(d, p-1) = 1$, then a^d is also a primitive root modulo p.

Solution

(a) A *primitive root modulo p* is an element a with order $e_p(a) = p - 1$; ie, such that the minimum power e such that $a^e \equiv_p 1$ is $e = p - 1$.
(b) $\phi(46) = \phi(2)\phi(23) = 22$.
(c) If a isn't primitive mod 13 then $a^6 \equiv_{13} 1$. Checking $2^6 \equiv_{13} -1$, so p is primitive.
(d) We need to show that the order $e = e_p(a^d)$ is $p - 1$. By Fermat's Little Theorem and the Order Divisibility Theorem, $e \mid p - 1$. On the other hand $1 \equiv_p (a^d)^e = a^{e \cdot d}$, so by the order divisiblity theorem, as $e_p(a) = p - 1$, we have $(p - 1) \mid e \cdot d$. As $\gcd(p - 1, d) = 1$, this implies $(p - 1) \mid e$; so $e = p - 1$, as needed.

(So anything in $\{2, 2^5, 2^7, 2^{11}\} = \{2, 6, 11, 7\}$ is an answer to (c).)