

Number Theory: iClicker Questions

Contents

1	01-31-2011	2
2	02-04-2011	19
3	2-7-2011	30
4	2-14-2011	39
5	03-07-11	50
6	03-31-2011	61
7	04-04-2011	70
8	04-12-2011	79
9	04-18-2011	92

1 01-31-2011

Question Suppose $b > a > 0$. Which of the following is not the same as $a|b$?

- A. A segment of length b can be divided a segments of the same integer length.
- B. The remainder in the division algorithm is zero
- C. There exists a q so that $a = bq$
- D. The fraction b/a can be reduced to an integer
- E. There is an integer solution x to the equation $b = ax$

Answer to Question Suppose $b > a > 0$. Which of the following is not the same as $a|b$?

- A. A segment of length b can be divided a segments of the same integer length.
- B. The remainder in the division algorithm is zero
- C. There exists a q so that $a = bq$ is the correct answer.**
- D. The fraction b/a can be reduced to an integer
- E. There is an integer solution x to the equation $b = ax$

Question Suppose $b > a > 0$ and $d = (a, b)$. Which of the following is not true?

A. $d|a$ and $d|b$.

B. If $c|a$ and $c|b$ then $c < d$.

C. If $c|a$ and $c|b$ then $c|d$.

D. $ax + by = d$

E. If $ax + by \neq 0$ then $|ax + by| \geq d$

Answer to Question Suppose $b > a > 0$ and $d = (a, b)$. Which of the following is not true?

A. $d|a$ and $d|b$.

B. If $c|a$ and $c|b$ then $c < d$. is the correct answer.

C. If $c|a$ and $c|b$ then $c|d$.

D. $ax + by = d$

E. If $ax + by \neq 0$ then $|ax + by| \geq d$

Note that D is also false for general x and y.

Question Which (if any) of A-D are false?

A. If $ac|bc$ and $c \neq 0$ then $a|b$

B. If n is odd then $8|n^2 - 1$

C. $4 \nmid n^2 + 2$

D. $(a, a+2)$ equals either 1 or 2

E. All are true

Answer to Question Which (if any) of A-D are false?

A. If $ac|bc$ and $c \neq 0$ then $a|b$

B. If n is odd then $8|n^2 - 1$

C. $4 \nmid n^2 + 2$

D. $(a, a+2)$ equals either 1 or 2

E. All are true is the correct answer.

Question How many steps are required by the Euclidean algorithm to show that $(47, 13) = 1$?

A. 3

B. 4

C. 5

D. 6

E. 7

Answer to Question How many steps are required by the Euclidean algorithm to show that $(47, 13) = 1$?

A. 3

B. 4

C. 5 is the correct answer.

D. 6

E. 7

Depending on when the algorithm terminates, it may be counted as 6 steps.

Question What is most significant in proving the Fundamental Theorem of Arithmetic?

- A. Proving that there exists a prime factorization
- B. Proving that nothing divides into a prime
- C. Proving that the prime factorization is unique up to the order of primes
- D. Proving that every number is divisible by a prime
- E. None of the above

Answer to Question What is most significant in proving the Fundamental Theorem of Arithmetic?

- A. Proving that there exists a prime factorization
- B. Proving that nothing divides into a prime
- C. Proving that the prime factorization is unique up to the order of primes is the correct answer.**
- D. Proving that every number is divisible by a prime
- E. None of the above

Question Which of the following A-D, is not a valid form for writing a positive integer a ?

A. $a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$

B. $a = \prod_{i=1}^k p_i^{\alpha_i}$

C. $a = \prod_{i=1}^{\infty} p_i^{\alpha_i}$

D. $a = \prod_p p^{\alpha(p)}$

E. All of the above are valid

Answer to Question Which of the following A-D, is not a valid form for writing a positive integer a ?

A. $a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$

B. $a = \prod_{i=1}^k p_i^{\alpha_i}$

C. $a = \prod_{i=1}^{\infty} p_i^{\alpha_i}$

D. $a = \prod_p p^{\alpha(p)}$

E. All of the above are valid is the correct answer.

Note that some of the α_i may be zero which means that the prime does not occur in the factorization.

Question If $a = \prod_{i=1}^{\infty} p_i^{\alpha_i}$ and $b = \prod_{i=1}^{\infty} p_i^{\beta_i}$. Then what is $[a, b]$?

A. $\prod_{i=1}^{\infty} p_i^{\beta_i} p_i^{\alpha_i}$

B. $\prod_{i=1}^{\infty} p_i^{|\beta_i \alpha_i|}$

C. $\prod_{i=1}^{\infty} p_i^{\min(\alpha_i, \beta_i)}$

D. $\prod_{i=1}^{\infty} p_i^{\max(\alpha_i, \beta_i)}$

E. None of the above

Answer to Question If $a = \prod_{i=1}^{\infty} p_i^{\alpha_i}$ and $b = \prod_{i=1}^{\infty} p_i^{\beta_i}$. Then what is $[a, b]$?

A. $\prod_{i=1}^{\infty} p_i^{\beta_i} p_i^{\alpha_i}$

B. $\prod_{i=1}^{\infty} p_i^{|\beta_i \alpha_i|}$

C. $\prod_{i=1}^{\infty} p_i^{\min(\alpha_i, \beta_i)}$

D. $\prod_{i=1}^{\infty} p_i^{\max(\alpha_i, \beta_i)}$ is the correct answer.

E. None of the above

Question The best way to find (a, b) is to find the prime factorization of a and the prime factorization of b to find the common factors.

A. True

B. False

C.

D.

E. I don't have an iClicker

Answer to Question The best way to find (a, b) is to find the prime factorization of a and the prime factorization of b to find the common factors.

A. True

B. False is the correct answer.

C.

D.

E. I don't have an iClicker

The best way is the Euclidean Algorithm, or, for very small numbers, to just consider common factors.

2 02-04-2011

Question If $a = \prod_{i=1}^{\infty} p_i^{\alpha_i}$ and $b = \prod_{i=1}^{\infty} p_i^{\beta_i}$. Then what is (a, b) ?

A. $\prod_{i=1}^{\infty} p_i^{\beta_i} p_i^{\alpha_i}$

B. $\prod_{i=1}^{\infty} p_i^{|\beta_i \alpha_i|}$

C. $\prod_{i=1}^{\infty} p_i^{\min(\alpha_i, \beta_i)}$

D. $\prod_{i=1}^{\infty} p_i^{\max(\alpha_i, \beta_i)}$

E. None of the above

Answer to Question If $a = \prod_{i=1}^{\infty} p_i^{\alpha_i}$ and $b = \prod_{i=1}^{\infty} p_i^{\beta_i}$. Then what is (a, b) ?

A. $\prod_{i=1}^{\infty} p_i^{\beta_i} p_i^{\alpha_i}$

B. $\prod_{i=1}^{\infty} p_i^{|\beta_i \alpha_i|}$

C. $\prod_{i=1}^{\infty} p_i^{\min(\alpha_i, \beta_i)}$ is the correct answer.

D. $\prod_{i=1}^{\infty} p_i^{\max(\alpha_i, \beta_i)}$

E. None of the above

Question If $a = \prod_{i=1}^k p_i^{\alpha_i}$ and $b = \prod_{i=1}^k p_i^{\beta_i}$. Then what is equivalent to $a|b$?

- A. $\alpha_i | \beta_i$ for all $i = 1, \dots, k$
- B. $\alpha_i \leq \beta_i$ for all $i = 1, \dots, k$
- C. $\alpha_i \leq \min\{\beta_1, \beta_2, \dots, \beta_k\}$
- D. $\alpha_i \leq \max\{\beta_1, \beta_2, \dots, \beta_k\}$
- E. None of the above

Answer to Question If $a = \prod_{i=1}^k p_i^{\alpha_i}$ and $b = \prod_{i=1}^k p_i^{\beta_i}$. Then what is equivalent to $a|b$?

A. $\alpha_i | \beta_i$ for all $i = 1, \dots, k$

B. $\alpha_i \leq \beta_i$ for all $i = 1, \dots, k$ is the correct answer.

C. $\alpha_i \leq \min\{\beta_1, \beta_2, \dots, \beta_k\}$

D. $\alpha_i \leq \max\{\beta_1, \beta_2, \dots, \beta_k\}$

E. None of the above

Question If a number between 1 and 10^{10} is chosen at random, a reasonable estimate on the probability that it is prime is roughly:

- A. 1 in 10^9
- B. 1 in 5000000
- C. 1 in 10000
- D. 1 in 500
- E. 1 in 25

Answer to Question If a number between 1 and 10^{10} is chosen at random, a reasonable estimate on the probability that it is prime is roughly:

A. 1 in 10^9

B. 1 in 5000000

C. 1 in 10000

D. 1 in 500

E. 1 in 25 is the correct answer.

There are $\pi(x)$ primes in the first x numbers so the ratio is $\pi(x)/x$ which is approximately $1/\ln(x)$

Question If $(a, p^2) = p$ and $(b, p^3) = p^2$ where p is a prime, then what is (ab, p^4) ?

- A. p
- B. p^2
- C. p^3
- D. p^4
- E. None of the above

Answer to Question If $(a, p^2) = p$ and $(b, p^3) = p^2$ where p is a prime, then what is (ab, p^4) ?

A. p

B. p^2

C. p^3 is the correct answer.

D. p^4

E. None of the above

Question If $(a, p^2) = p$ and $(b, p^3) = p^2$ where p is a prime, then what is $(a + b, p^4)$?

- A. p
- B. p^2
- C. p^3
- D. It depends...
- E. None of the above

Answer to Question If $(a, p^2) = p$ and $(b, p^3) = p^2$ where p is a prime, then what is $(a + b, p^4)$?

A. p is the correct answer.

B. p^2

C. p^3

D. It depends...

E. None of the above

3 2-7-2011

Question If $m|(a - b)$ and $m|(c - d)$ then $m|(ac - bd)$.

A. True

B. False

C.

D.

E.

Answer to Question If $m|(a - b)$ and $m|(c - d)$ then $m|(ac - bd)$.

A. True is the correct answer.

B. False

C.

D.

E.

Question A complete residue system modulo 9 is

A. 1, 3, 5, 7, 9, 11, 13, 15, 17

B. $-6, -5, -4, -3, -2, -1, 0, 1, 2$

C. 9, 10, 11, 12, 13, 14, 15, 16, 17

D. All of the above

E. None of the above

Answer to Question A complete residue system modulo 9 is

A. 1, 3, 5, 7, 9, 11, 13, 15, 17

B. $-6, -5, -4, -3, -2, -1, 0, 1, 2$

C. 9, 10, 11, 12, 13, 14, 15, 16, 17

D. All of the above is the correct answer.

E. None of the above

Question A reduced residue system modulo 10 is

- A. 1, 4, 5, 6, 7, 8, 9
- B. 1, 3, 5, 7, 9
- C. 1, 3, 4, 7, 8, 9
- D. All of the above
- E. None of the above

Answer to Question A reduced residue system modulo 10 is

A. 1, 4, 5, 6, 7, 8, 9

B. 1, 3, 5, 7, 9

C. 1, 3, 4, 7, 8, 9

D. All of the above

E. None of the above is the correct answer.

A reduced residue system would be 1, 3, 7, 9 and $\phi(10) = 4$

Question If $(n, 15) = 1$, what is n^{10} congruent to modulo 15?

A. 1

B. n

C. n^2

D. n^3

E. None of the above

Answer to Question If $(n, 15) = 1$, what is n^{10} congruent to modulo 15?

A. 1

B. n

C. n^2 is the correct answer.

D. n^3

E. None of the above

By counting we get that $\phi(15) = 8$ so $n^8 \equiv 1 \pmod{15}$ so

$$n^{10} = n^8 n^2 \equiv 1 \cdot n^2 \pmod{15}$$

4 2-14-2011

Question If p is an odd prime then what is $(p - 2)!$ congruent to modulo p

- A. 1
- B. -1
- C. $p - 2$
- D. It depends on p
- E. None of the above

Answer to Question If p is an odd prime then what is $(p - 2)!$ congruent to modulo p

A. 1 is the correct answer.

B. -1

C. $p - 2$

D. It depends on p

E. None of the above

This was shown in the course of proving Wilson's Theorem.

We can also derive it from Wilson's Theorem as follows.

Since $(p - 1)! \equiv -1 \pmod{p}$ then $(p - 2)!(p - 1) \equiv -1 \pmod{p}$ so $(p - 2)!(-1) \equiv -1 \cdot 1 \pmod{p}$ and the -1 can be canceled from both sides since $(-1, p) = 1$

Question To find a solution x to $ax \equiv b \pmod{m}$ the best way to proceed is to:

- A. Set $x = b/a$.
- B. Try all numbers x between 0 and $m - 1$
- C. Use the division algorithm
- D. Use the Euclidean Algorithm
- E. None of the above

Answer to Question To find a solution x to $ax \equiv b \pmod{m}$ the best way to proceed is to:

- A. Set $x = b/a$.
- B. Try all numbers x between 0 and $m - 1$
- C. Use the division algorithm
- D. Use the Euclidean Algorithm is the correct answer.**
- E. None of the above

We use the Euclidean Algorithm to solve $ax + my = b$ for integers x and y and note that this implies $b - ax = my$ so $m|(b - ax)$ which means $ax \equiv b \pmod{m}$

Question How many solutions are there to the congruence $15x = 25 \pmod{35}$?

- A. 1
- B. 5
- C. 15
- D. Infinitely many
- E. None of the above

Answer to Question How many solutions are there to the congruence $15x = 25 \pmod{35}$?

- A. 1
- B. 5 is the correct answer.**
- C. 15
- D. Infinitely many
- E. None of the above

We just count the number of solutions, incongruent, modulo 35. The 5 comes from the greatest common divisor of 5 and 35.

Question Find all incongruent solutions to $15x = 25 \pmod{35}$

- A. 4
- B. 4, 9, 14, 19, 24
- C. 4, 11, 18, 25, 32
- D. 4, 39, 74, 109, 144
- E. None of the above

Answer to Question Find all incongruent solutions to $15x = 25 \pmod{35}$

A. 4

B. 4, 9, 14, 19, 24

C. 4, 11, 18, 25, 32 **is the correct answer.**

D. 4, 39, 74, 109, 144

E. None of the above

Question For a, b, c positive integers, consider the tasks:

1. Find x so $0 \equiv c - ax \pmod{b}$
2. Find x so $ax \equiv c \pmod{b}$
3. Find x and y so $ax + by = c$

What is the difference between the above?

- A. 1 and 2 are essentially the same, 3 is different
- B. 1 and 3 are essentially the same, 2 is different
- C. 2 and 3 are essentially the same, 1 is different
- D. All are essentially the same
- E. All are different

Answer to Question For a, b, c positive integers, consider the tasks:

1. Find x so $0 \equiv c - ax \pmod{b}$
2. Find x so $ax \equiv c \pmod{b}$
3. Find x and y so $ax + by = c$

What is the difference between the above?

- A. 1 and 2 are essentially the same, 3 is different
- B. 1 and 3 are essentially the same, 2 is different
- C. 2 and 3 are essentially the same, 1 is different
- D. All are essentially the same is the correct answer.**
- E. All are different

5 03-07-11

Question Which is (probably) slowest.

- A. Find a large “probable” prime with about 10 digits.
- B. Find (m, n) for 10 digit integers m and n .
- C. Find the least non-negative residue of a^n modulo m where a, m, n are all about 10 digits.
- D. Factor a number which is a product of two 10 digit primes
- E. Solve $ax \equiv b \pmod{m}$ for x where a, b, m are all about 10 digits.

Answer to Question Which is (probably) slowest.

- A. Find a large “probable” prime with about 10 digits.
- B. Find (m, n) for 10 digit integers m and n .
- C. Find the least non-negative residue of a^n modulo m where a, m, n are all about 10 digits.
- D. Factor a number which is a product of two 10 digit primes is the correct answer.**
- E. Solve $ax \equiv b \pmod{m}$ for x where a, b, m are all about 10 digits.

Note that factoring in general is much much much slower than the other tasks. Also note that B is almost the same as E.

Question To make it “hard” for someone to find primes $p > 1$ and $q > 1$ given their product $m = p \cdot q$ which is least important?

- A. Make sure to keep p, q secret.
- B. Make both p and q large
- C. Make sure that m is not of the form $6k + 5$
- D. Make sure that m is not a perfect square.
- E. Make p, q large primes so that $(p - 1)/2$ and $(q - 1)/2$ are prime.

Answer to Question To make it “hard” for someone to find primes $p > 1$ and $q > 1$ given their product $m = p \cdot q$ which is least important?

- A. Make sure to keep p, q secret.
- B. Make both p and q large
- C. Make sure that m is not of the form $6k + 5$ is the correct answer.**
- D. Make sure that m is not a perfect square.
- E. Make p, q large primes so that $(p - 1)/2$ and $(q - 1)/2$ are prime.

Note that something like E is important to prevent factorization by the Pollard $p - 1$ method.

Question For $n > 0$ we have that $5|(n^4 + 4^n)$ if and only if

- A. n is any positive integer
- B. n is odd
- C. $5|n$
- D. 5 does not divide n
- E. 5 does not divide n and n is odd.

Answer to Question For $n > 0$ we have that $5|(n^4 + 4^n)$ if and only if

A. n is any positive integer

B. n is odd

C. $5|n$

D. 5 does not divide n

E. 5 does not divide n and n is odd. is the correct answer.

- Note that if $n|5$ then $n^4 \equiv 0 \pmod{5}$ and if 5 does not divide n then $n^4 \equiv 1 \pmod{5}$ by Fermat's Little Theorem.
- Note that if n is odd $4^n \equiv -1 \pmod{5}$ and if n is even $4^n \equiv 1 \pmod{5}$.
- The answer is E from adding the various cases above to see when $n^4 + 4^n \equiv 0 \pmod{5}$

Question To factor a number n which is least likely to be helpful?

- A. Find large a and b so $n = ax + b$
- B. Find $a, b > 1$ so $n = ab$
- C. Find an m so $1 < (m, n) < n$
- D. Find $a, b > 0$ so $n = a^2 - b^2$
- E. Find $a, b > 0$ so $a^2 \equiv b^2 \pmod{n}$

Answer to Question To factor a number n which is least likely to be helpful?

A. Find large a and b so $n = ax + b$ is the correct answer.

B. Find $a, b > 1$ so $n = ab$

C. Find an m so $1 < (m, n) < n$

D. Find $a, b > 0$ so $n = a^2 - b^2$

E. Find $a, b > 0$ so $a^2 \equiv b^2 \pmod{n}$

Parts D and E are frequently used to help factor since $a^2 - b^2$ factors into $(a - b) \cdot (a + b)$.

Note that E will produce a non-trivial factorization if $a \not\equiv \pm b \pmod{n}$.

Question If n is odd then $4^n - n^4 = a^2 - b^2$ where $a = 2^n + n^2$ and b is

A. Impossible to find

B. 42

C. $2 \cdot 2^n n^2$

D. $2^{(n+1)/2} n$

E. $2^{n/2} n$

Answer to Question If n is odd then $4^n - n^4 = a^2 - b^2$ where $a = 2^n + n^2$ and b is

A. Impossible to find

B. 42

C. $2 \cdot 2^n n^2$

D. $2^{(n+1)/2} n$ is the correct answer.

E. $2^{n/2} n$

6 03-31-2011

Question The order of 2 modulo 7 is

A. 6

B. 3

C. 2

D. 1

E. 4

Answer to Question The order of 2 modulo 7 is

A. 6

B. 3 is the correct answer.

C. 2

D. 1

E. 4

Note that even though $2^6 \equiv 1$ modulo 7, it does not follow that 6 is the order because 6 is not the smallest exponent that we can use.

Question How many primitive roots does 7 have?

A. 5

B. 4

C. 3

D. 2

E. 1

Answer to Question How many primitive roots does 7 have?

A. 5

B. 4

C. 3

D. 2 is the correct answer.

E. 1

$\phi(\phi(7)) = \phi(6) = \phi(3)\phi(2) = 2 \cdot 1 = 2$ is the number of primitive roots

Question Which of the following is a primitive root of 7 ?

A. 1

B. 2

C. 3

D. 4

E. 6

Answer to Question Which of the following is a primitive root of 7?

A. 1

B. 2

C. 3 is the correct answer.

D. 4

E. 6

1. Note that we saw earlier that 2 had order 3 so it is not a primitive root.

2. Also 1 cannot be primitive roots as 1 has order 1 modulo any prime p

3. Note that 6 cannot be a primitive root, since for any prime p ,

$$p - 1 \equiv -1 \pmod{p} \text{ and so } (p - 1)^2 \equiv (-1)^2 \equiv 1 \pmod{p}.$$

So the order of $p - 1$ modulo p is 2 for $p \geq 3$. And for primes $p > 3$, $p - 1$ is not a primitive root as its order is less than $p - 1$.

4. In addition to 3, the other primitive root modulo 7 is 5.

Question Suppose $(a, m) = 1$. Which is (closest to) a necessary and sufficient condition to establish that the order of a modulo m is equal to h ?

- A. Show that $a^h \equiv 1 \pmod{m}$
- B. Show that $a^h \equiv 1 \pmod{m}$ and $a^k \not\equiv 1 \pmod{m}$ for $1 < k < h$
- C. Show that $a^h \equiv 1 \pmod{m}$ and $a^k \not\equiv 1 \pmod{m}$ for $k|h$ and $k > 1$
- D. Show that $(a, h) = 1$
- E. Show that m is prime

Answer to Question Suppose $(a, m) = 1$. Which is (closest to) a necessary and sufficient condition to establish that the order of a modulo m is equal to h ?

A. Show that $a^h \equiv 1 \pmod{m}$

B. Show that $a^h \equiv 1 \pmod{m}$ and $a^k \not\equiv 1 \pmod{m}$ for $1 < k < h$

C. Show that $a^h \equiv 1 \pmod{m}$ and $a^k \not\equiv 1 \pmod{m}$ for $k|h$ and $k > 1$ is the correct answer.

D. Show that $(a, h) = 1$

E. Show that m is prime

1. Part A is not sufficient and B is not necessary, we can simplify it to part C.
2. Part E just says that m has primitive roots, nothing about the order of any particular element.

7 04-04-2011

Question Which of the following moduli do not have primitive roots?

A. 14

B. 50

C. 35

D. 18

E. 29

Answer to Question Which of the following moduli do not have primitive roots?

A. 14

B. 50

C. 35 is the correct answer.

D. 18

E. 29

1. $14 = 7 \cdot 2$

2. $50 = 5^2 \cdot 2$

3. $35 = 5 \cdot 7$

4. $18 = 3^2 \cdot 2$

5. 29 is prime

Question Which of the following moduli do have primitive roots?

- A. 6
- B. 128
- C. 35
- D. 52
- E. 98

Answer to Question Which of the following moduli do have primitive roots?

A. 6

B. 128

C. 35

D. 52

E. 98 is the correct answer.

1. $6 = 3 \cdot 2$

2. $128 = 2^7$

3. $35 = 5 \cdot 7$

4. $52 = 4 \cdot 13$

5. $98 = 7^2 \cdot 2$

Question How many distinct primitive roots modulo 18 are there?

A. 6

B. 4

C. 3

D. 2

E. None of the above

Answer to Question How many distinct primitive roots modulo 18 are there?

A. 6

B. 4

C. 3

D. 2 is the correct answer.

E. None of the above

$$\phi(\phi(18)) = \phi(\phi(2)\phi(9)) = \phi(1 \cdot \phi(9)) = \phi(3^2 - 3) = \phi(6) = \phi(3)\phi(2) = 2 \cdot 1$$

Question How many distinct primitive roots modulo 49 are there?

- A. 12
- B. 10
- C. 8
- D. 6
- E. None of the above

Answer to Question How many distinct primitive roots modulo 49 are there?

A. 12 is the correct answer.

B. 10

C. 8

D. 6

E. None of the above

$$\phi(\phi(49)) = \phi(7^2 - 7) = \phi(42) = \phi(6)\phi(7) = 2 \cdot 6 = 12$$

8 04-12-2011

Question Suppose p is an odd prime and $(a, p) = 1$. How does one go about finding out if $a^{(p-1)/2} \equiv 1 \pmod{p}$?

- A. Compute $a^{(p-1)/2}$, then divide it by p and see if the remainder is equal to 1
- B. This is always true, so there is no need to check
- C. Check to see if it is equal to -1 , if not, then it is 1.
- D. Use modular exponentiation
- E. None of the above

Answer to Question Suppose p is an odd prime and $(a, p) = 1$.
How does one go about finding out if $a^{(p-1)/2} \equiv 1 \pmod{p}$?

A. Compute $a^{(p-1)/2}$, then divide it by p and see if the remainder is equal to 1

B. This is always true, so there is no need to check

C. Check to see if it is equal to -1 , if not, then it is 1.

D. Use modular exponentiation is the correct answer.

E. None of the above

1. Note that while A is theoretically valid, it would take a ludicrous amount of time and computer memory and storage space for large primes p and moderately large values of a .

2. C is also theoretically valid, but again is useless if done directly.

Question How long does it take for modular exponentiation to find if $a^{(p-1)/2} \equiv 1 \pmod{p}$ for reasonably large values of a and p ?

- A. Real fast, not quite as fast as the speed of light, but it is really close.
- B. You gotta wait until the sun burns out! Five times!!!
- C. Exactly $M(9)$ seconds, where $M(9)$ is the 9th Mersenne prime.
- D. It's fast but it takes about $10^{10000000000000}$ tera-bytes of memory.
- E. It's pretty quick, like about $\log_2(p)$ steps, and just about enough memory to hold a number the size of p^2 with some left over to work on stuff.

Answer to Question How long does it take for modular exponentiation to find if $a^{(p-1)/2} \equiv 1 \pmod{p}$ for reasonably large values of a and p ?

- A. Real fast, not quite as fast as the speed of light, but it is really close.
- B. You gotta wait until the sun burns out! Five times!!!
- C. Exactly $M(9)$ seconds, where $M(9)$ is the 9th Mersenne prime.
- D. It's fast but it takes about $10^{10000000000000}$ tera-bytes of memory.
- E. It's pretty quick, like about $\log_2(p)$ steps, and just about enough memory to hold a number the size of p^2 with some left over to work on stuff. is the correct answer.**

Question Solving $x^2 - 6x + 13 \equiv 0 \pmod{17}$ for x is the same as

- A. Solving $w^2 \equiv -4 \pmod{17}$ for w and letting $x = w + 3$
- B. Solving $w^2 \equiv 4 \pmod{17}$ for w and letting $x = w + 3$
- C. Solving $w^2 \equiv 4 \pmod{16}$ for w and letting $x = w + 3$
- D. Solving $w^2 \equiv -4 \pmod{16}$ for w and letting $x = w + 3$
- E. None of the above

Answer to Question Solving $x^2 - 6x + 13 \equiv 0 \pmod{17}$ for x is the same as

- A. Solving $w^2 \equiv -4 \pmod{17}$ for w and letting $x = w + 3$ is the correct answer.**
- B. Solving $w^2 \equiv 4 \pmod{17}$ for w and letting $x = w + 3$
- C. Solving $w^2 \equiv 4 \pmod{16}$ for w and letting $x = w + 3$
- D. Solving $w^2 \equiv -4 \pmod{16}$ for w and letting $x = w + 3$
- E. None of the above

$$x^2 - 6x + 13 = x^2 - 6x + 9 - 9 + 13 = (x - 3)^2 + 4$$

Question Suppose m is positive. Saying a is a quadratic residue modulo m is equivalent to which of the following:

A. $(a, m) = 1$

B. $(a, (a, m)) = 1$

C. $(a, m) = 1$ and there exists an x so $x^2 \equiv a \pmod{m}$

D. $(a, m) = 1$ and $a^{(m-1)/2} \equiv -1 \pmod{m}$

E. None of the above

Answer to Question Suppose m is positive. Saying a is a quadratic residue modulo m is equivalent to which of the following:

A. $(a, m) = 1$

B. $(a, (a, m)) = 1$

C. $(a, m) = 1$ and there exists an x so $x^2 \equiv a \pmod{m}$ is the correct answer.

D. $(a, m) = 1$ and $a^{(m-1)/2} \equiv -1 \pmod{m}$

E. None of the above

1. Part D may not make sense because m may not be odd (or prime).
2. Note that part C is the definition of quadratic residue.

Question Suppose p is an odd prime and $(a, p) = 1$. Saying a is a quadratic non-residue modulo p is equivalent to which of the following:

A. $a^{(p-1)/2} \equiv 1 \pmod{p}$

B. $a^{(p-1)/2} \equiv -1 \pmod{p}$

C. $a^{(p-1)/4} \equiv -1 \pmod{p}$

D. $a^{(p-1)/4} \equiv 1 \pmod{p}$

E. None of the above

Answer to Question Suppose p is an odd prime and $(a, p) = 1$. Saying a is a quadratic non-residue modulo p is equivalent to which of the following:

A. $a^{(p-1)/2} \equiv 1 \pmod{p}$

B. $a^{(p-1)/2} \equiv -1 \pmod{p}$ is the correct answer.

C. $a^{(p-1)/4} \equiv -1 \pmod{p}$

D. $a^{(p-1)/4} \equiv 1 \pmod{p}$

E. None of the above

This is Euler's criteria and is quickly accomplished using modular exponentiation.

Question Suppose p is an odd prime and $(a, p) = 1$. Saying a is a quadratic residue modulo p is equivalent to which of the following:

A. $a^{(p-1)/2} \equiv 1 \pmod{p}$

B. $a^{(p-1)/2} \equiv -1 \pmod{p}$

C. $a^{(p-1)/4} \equiv -1 \pmod{p}$

D. $a^{(p-1)/4} \equiv 1 \pmod{p}$

E. None of the above

Answer to Question Suppose p is an odd prime and $(a, p) = 1$. Saying a is a quadratic residue modulo p is equivalent to which of the following:

A. $a^{(p-1)/2} \equiv 1 \pmod{p}$ **is the correct answer.**

B. $a^{(p-1)/2} \equiv -1 \pmod{p}$

C. $a^{(p-1)/4} \equiv -1 \pmod{p}$

D. $a^{(p-1)/4} \equiv 1 \pmod{p}$

E. None of the above

This is Euler's criteria and is quickly accomplished using modular exponentiation.

9 04-18-2011

Question If p and q are distinct odd primes, then the Legendre symbol $\left(\frac{p}{q}\right)$ is equal to

- A. 1 if $x^2 \equiv q \pmod{p}$ has a solution x
- B. 1 if $x^2 \equiv p \pmod{q}$ has a solution x
- C. -1 if $x^2 \equiv p \pmod{q}$ has a solution x
- D. -1 if $x^2 \equiv q \pmod{p}$ has a solution x
- E. None of the above

Answer to Question If p and q are distinct odd primes, then the Legendre symbol $\left(\frac{p}{q}\right)$ is equal to

A. 1 if $x^2 \equiv q \pmod{p}$ has a solution x

B. 1 if $x^2 \equiv p \pmod{q}$ has a solution x is the correct answer.

C. -1 if $x^2 \equiv p \pmod{q}$ has a solution x

D. -1 if $x^2 \equiv q \pmod{p}$ has a solution x

E. None of the above

Question If p and q are distinct odd primes, then the Legendre symbol $\left(\frac{p}{q}\right)$ is equal to

A. $(-1)^{(p-1)(q-1)} \left(\frac{q}{p}\right)$

B. $(-1)^{p-1}(-1)^{q-1} \left(\frac{q}{p}\right)$

C. $(-1)^{(p-1)/2}(-1)^{(q-1)/2} \left(\frac{q}{p}\right)$

D. $(-1)^{(p-1)(q-1)/4} \left(\frac{q}{p}\right)$

E. None of the above

Answer to Question If p and q are distinct odd primes, then the Legendre symbol $\left(\frac{p}{q}\right)$ is equal to

A. $(-1)^{(p-1)(q-1)} \left(\frac{q}{p}\right)$

B. $(-1)^{p-1}(-1)^{q-1} \left(\frac{q}{p}\right)$

C. $(-1)^{(p-1)/2}(-1)^{(q-1)/2} \left(\frac{q}{p}\right)$

D. $(-1)^{(p-1)(q-1)/4} \left(\frac{q}{p}\right)$ is the correct answer.

E. None of the above

Question The Legendre symbol $\left(\frac{4}{7}\right)$ is equal to

A. 1

B. -1

C. 0

D. 17

E. None of the above

Answer to Question The Legendre symbol $\left(\frac{4}{7}\right)$ is equal to

A. 1 is the correct answer.

B. -1

C. 0

D. 17

E. None of the above

This is simple, because 4 is a perfect square.

Question The Legendre symbol $\left(\frac{7}{37}\right)$ is equal to

- A. 1
- B. -1
- C. 0
- D. 17
- E. None of the above

Answer to Question The Legendre symbol $\left(\frac{7}{37}\right)$ is equal to

A. 1 is the correct answer.

B. -1

C. 0

D. 17

E. None of the above

$$\left(\frac{7}{37}\right) = \left(\frac{37}{7}\right) = \left(\frac{2}{7}\right) = (-1)^{(7^2-1)/8} = 1$$