**Problem Set 3**

**Problem 1.**

**a)** Use the Pulverizer to find integers and such that

|  |  |  |  |
| --- | --- | --- | --- |
| n | k | r | r (linear combo) |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**b)** Use the previous part to find the inverse of 59 modulo 135 in the range {1,…,134}.

**c)** Use Euler’s theorem to find the inverse of 17 modulo 31 in the range {1,…,30}

**d)** Find the remainder of divided by 83.

**Problem 2**. Prove the following statements, assuming all numbers are positive integers.

**a)** If , then

*Proof.* If then for some integer . Through substitution we get Then and we are done. ∎

**b)** If and , then .

*Proof*. If then for some integer , , similarly for some integer . By substitution

Then and we are done.

**c)**

*Proof*. By chain of *iff-*statements. First, for some integer . Then, And finally, . ∎

**d)**

*Proof.* By theorem 4.2.1, can be written as the smallest positive linear combination . Then and translating back into gcd notation using the theorem, . ∎

**Problem 3.** In this problem, we will investigate numbers which are squares modulo a prime number .

**a)** An integer is **square modulo**  if there exists another integer such that . Prove that if and only if or .

*Proof*. By a chain of *iff-*statements. By the definition of congruence, if and only if , which can be written as . This is then true if and only if or . Again by the definition of congruence, both statements can be rewritten as or . ∎

**b)** There is a simple test we can perform to see if a number is a square modulo . It states that

**Theorem 1** (Euler’s Criterion):

Prove the first part of Euler’s Criterion.

*Proof*. As defined in part *a*, if is square modulo , then there exists an integer such that . Using Fermat’s Little Theorem, . This could be rewritten as Substituting back for gives completing the proof.

**c)** Assume that and . Given and , find one possible value of .

By definition is square modulo , so by Euler’s Criterion, We can then multiply both sides by such that . Since can be written as , the exponent of is even, and taking the square root of it gives as a solution for

**Problem 4.** Prove that for any prime, , and integer, ,

where is Euler’s function.

*Proof*. The only prime factor of is . Then, by Euler’s Theorem,

**Problem 5.** Start with two distinct positive ints, . On each player’s turn, they write a new positive int that is a common divisor of two numbers that are already there. If a player cannot play, then they lose.

**a)** Show that every number on the board at the end of the game is either or a positive divisor of .

First, and begin on the board.

Then, by Property 1 of Lemma 4.2.4, every common divisor of and divides . So all common divisors of the starting values and divide .

The remaining numbers that are possible to list are common divisors of the common divisors of the starting values. But these numbers are already divisors of the starting values, so this provides no new values.

**b)** Show that every positive divisor of is on the board at the end of the game.

By the rules of the game, assuming both players notice all possible common divisors, the game isn’t over until all of the common divisors of have been found. Since is one of those divisors, all of its divisors are also divisors of , thus they have all been found by the end of the game.

**c)** Describe a strategy that lets you win the game every time.

If there are an even number of common divisors, then the second player will win. If there are an odd number of divisors, then the first player will win. But how do you know if there are an even or odd number of divisors?

The total number of divisors is equal to the total number of factors of plus one. But then how do you factor for large numbers? We know that’s as good as impossible, since it’s used in cryptography. But is there a way to know how many factors there are? Nope. Stack exchange says no. There are upper bounds, but that helps nothing with the parity of the number of factors. Maybe I’m just supposed to assume this number is factorable?

**Problem 6.** In one of the previous problems, you calculated square roots of numbers modulo primes equivalent to 3 modulo 4. In this problem you will prove that there are an infinite number of such primes!

**a)** As a warm-up, prove that there are an infinite number of prime numbers.

*Proof*. By contradiction. Assume the statement is false, that there exists a set for all prime numbers that is finite, that is We can then imagine a prime number that is the result of multiplying all of the prime numbers in the set and then adding 1. This prime number , however, is not in the set of all prime numbers, therefore there is a contradiction and the statement is true.

**b)** Prove that if is an odd prime, then or .

*Proof*. Modulus 4 divides numbers into four sets: numbers for which

, for which

, for which

, and for which

.

The remainder of 4 and an odd number must be odd, which means odd numbers, including odd primes, fall into the sets and

**c)** Prove that if , then has a prime factor

*Proof*. Proof by contradiction. Assume that does not have a prime factor . Since, as proven in part b, all odd primes are either or must have a prime factorization of all primes such that . It would not have the even prime, 2, because when divided by 4 it gives an odd remainder. Each of the primes in ’s prime factorization could then be written in the form , for some integer . However, if you take any two numbers of the form , such that

then the product is also of the form . This means that , the product of its prime factorization, would be of the pattern , and thus, . But this is a contradiction, therefore must have a prime factor .

**d)** Let be the set of all primes such that Prove by contradiction that has an infinite number of primes.

*Proof*. By contradiction. Assume that there exists a set for all primes such that that is finite, that is We can then define a number . Since is one less than any number divisible by any of the numbers in the set , it is not divisible by any numbers in the set . We can then say that there is a number of the pattern . This is the same as a number congruent to modulus 4. By part c, has a prime factor . Since we know has no factors in the set , must be a prime number such that that is not in , hence there is a contradiction and we are done.