

HOMEWORK SOLUTIONS

Homework 1:

1. show if $a|b$ and $c|d$ then $ac|bd$.

2. what is $gcd(3636, 5418)$. Write your answer as a linear combination of 3636 and 5418.

3. Prove that $gcd(a,b,c) = gcd(gcd(a,b),c)$. Use this to calculate $gcd(1456, 819, 1092)$.

4. If $gcd(a,b)=d$ then what is $gcd(a/d,b/d)$? Prove your answer.

5. Prove that $\sqrt{2}$ is irrational. (Hint: assume it is rational and get a contradiction.)

Homework 2:

1. If $a|b$ and $c|d$ then $b = na, d = mc$ for some integers $n, m$. Then $bd = namb = nmac$ and thus $ac|bd$.

2. If $d = gcd(a,b,c)$ and $e = gcd(gcd(a,b),c)$. We will show that $d|e$ and $e|d$ and therefore $e = d$. By definition $e|gcd(a,b),c$ and therefore $e|a,b$. Thus $e|a,b,c$ and thus $e$ is a common divisor of $a,b,c$ and so by definition of $d, e \leq d$. By definition $d|a,b,c$. We now show the following:

   \[
   if \ d|a,b, \ then \ d|gcd(a,b). \]

   (6)

   One way to do this is to use theorem 4 which says that $gcd(a,b) = ua + vb$ for some integers $u$ and $v$. But then since $d|a,b$ we have $d$ divides any linear combination of $a$ and $b$ which means $d|gcd(a,b)$. Thus $d$ is a common divisor of $gcd(a,b)$ and $c$ and therefore $d \leq e$.

4. Let $e = gcd(a/d, b/d)$ then $e|a/b, b/d$ and so $ed|a,b$. Thus $ed$ is less than or equal to $gcd(a,b) = d$ and so $e = 1$.

5. Assume $\sqrt{2}$ is rational so that we can write $\sqrt{2} = a/b$ with $gcd(a,b) = 1$. Then $b\sqrt{2} = a$ so that $b^2 = a^2$. Thus $a^2$ is even which makes $a$ even. Writing $a = 2a'$ we see that $b^2 = 4(a')^2$ and so $b^2 = 2(a')^2$ which implies $a$ is even as well. But then 2 is a common divisor of $a$ and $b$ which contradicts $gcd(a,b) = 1$. Thus $\sqrt{2}$ cannot be rational.

Homework 2

1. Your favorite food comes in three sizes: 6-pack, 9-pack or 20-pack. What is the largest amount of your favorite food that you can’t get from a combination of these packs.

2. Prove that for every integer $n$, $n^2 + n$ is even. Show that for every integer $n$, there exist integers $p$ and $q$ so that $n = p - q$ and $n^2 = p + q$.

3. Prove there are no prime numbers $a, b$ and $c$ such that $a^3 + b^3 = c^3$. 


1. We notice that looking at this problem with an eye towards remainders when dividing by 6 is helpful. First notice that be using just the 6-pack, we can get all multiples of 6. Then notice that by using one 9-pack and multiple 6-packs we can get every number that is 9 or above that has a remainder 3 when divided by 6. Similarly, we can get every number 20 or above that has remainder 2 when divided by 6. We can get every number 29 or above that has remainder 1 when divided by 6. Finally we can get any number 49 and above that has a remainder 1 when divided by 6. In this way we see that no matter what the remainder of the number is when divided by 6, if it is above 49 we can get it. That leaves 43 as the last number we could not get.

2. We have \( n^2 + n = n(n + 1) \) a product of consecutive numbers. If \( n \) is odd then \( n + 1 \) is even and so is \( n(n + 1) \), likewise if \( n \) is even so is \( n(n + 1) \) so either way \( n(n + 1) = n^2 + n \) is even. (Alternatively you could do two cases: \( n = 2k \) or \( n = 2k + 1 \) and verify in both those cases that \( n^2 + n \) has a factor of two.

For the second part set \( p = \frac{n^2 + n}{2} \), \( q = \frac{n^2 - n}{2} \). It is easy to check that \( p + q = n^2 \) and \( p - q = n \). We NEED to show \( p \) and \( q \) are integers. \( p \) is an integer since \( n^2 + n \) is even. Since \( q = p - n \) with \( p \) and \( n \) integers, \( q \) must be an integer as well.

3. If we just look at the possibilities for the combinations of even and odd numbers we see there are four possibilities: i) \( a, b, c \) are all even, ii) \( a \) even, \( b, c \) odd, iii) \( b \) even, \( a, c \) odd or iv) \( c \) even, \( a, b \) odd. The cases ii) and iii) are the same with the roles of \( a \) and \( b \) switched. The only even prime is 2. Therefore for case i) we have to only check that \( 2^3 + 2^3 \neq 2^3 \). For case ii) we ask whether odd primes \( b, c \) exist so that \( 8 + b^3 = c^3 \) or \( c^3 - b^3 = (c - b)(c^2 + cb + b^2) = 8. \) But \( c^2 + cb + b^2 \geq 3^2 + 33 + 3^2 \) since \( b, c \) need to be odd primes which is impossible since it is bigger than 8. Finally, for case iv) we are looking for odd primes \( a, b \) such that \( a^3 + b^3 = 8 \). This is clearly impossible since the left and side must be at least 54.

Homework 3.

1. I’m getting a new 212 phone number. . . what is the chance (approximately) that it is prime?

2. Prove that there exists a sequence of \( n \) consecutive composite numbers for each \( n \).

3. Consider \( n^2 + n + 41 \). Are any of the first ten such numbers not prime? Find a value for \( n \) for which this is not prime. No calculators allowed for this.

4. Write a summary (no more than a page) of what you’ve learned so far highlighting the important ideas.

1. We use the theorem that says that \( \pi(x) \approx \frac{x}{\log x} \). This problem is asking for the percentage of primes between 2120000000 and 2129999999. This is the expression:

\[
\frac{\pi(2129999999) - \pi(2120000000)}{2129999999 - 2120000000}.
\]

Then you use the approximation for the \( \pi(x) \) to get an approximate answer.

2. Here are two proofs.

A) Consider the sequence of \( n - 1 \) consecutive integers \( n! + 2, n! + 3, n! + 4, \ldots, n! + n. \) We have \( n! + i = i(n - 1) \ldots (i + 1)(i - 1) \ldots 1 + 1 \) so therefore for \( 2 \leq i \leq n, n! + i \) is composite.

B) Proof by contradiction. Suppose there was an \( N \) so that there were not \( N \) consecutive composites anywhere. That would mean that for every string of \( N \) numbers, at least one of the numbers would be prime. Thus at least one in every \( N \) numbers would be prime and therefore \( \frac{\pi(x)}{x} \geq \frac{1}{N} \). But this can’t be true since \( \lim_{x \to \infty} \frac{\pi(x)}{x} = \lim_{x \to \infty} \frac{1}{\log x} = 0. \)

3. When \( n = 41 \) this is \( 41^2 + 41 + 41 \) which is clearly divisible by 41 so it can’t be prime.

Homework 4.

1. Use the fact that \( 1000 = -1 \mod 7 \) to develop a divisibility rule for 7. Use this rule to produce a number with at least 8 digits with no 7’s that is divisible by 7.

2. What is \( 2^{100} \mod 10? \)

3. What is \( 9! \mod 10? \)
1. The number with digits \( a_0a_{k-1} \ldots a_0 \), is equal to \( a_0 + 10a_1 + 10^2a_2 + \cdots + 10^k a_k \). Since \( 10 \equiv 3 \mod 7 \), \( 10^2 \equiv 9 \equiv 2 \mod 7 \) and \( 10^3 \equiv 8 \equiv -1 \mod 7 \) the number mod 7 can be computed by

- From left to right, group the digits in groups of 6.
- For each group (denote them \( b_3b_4 \ldots b_0 \)) compute \( (b_0 - b_3) + 3(b_1 - b_4) + 2(b_2 - b_6) \). Add these up for each group.
- If this number is divisible by 7 then the original number is divisible by 7.

To answer the second part you can just right down any 8 digit number and then use the rule above to figure out what the ninth digit would be to work. For instance if the last eight digits are 12345689 and we want \( c_{12345689} \) to be the number with digits \( a_0a_{k-1} \ldots a_0 \) equal to \( 12345689 \), then either

\[
\begin{align*}
10^2 & \equiv 9 \mod 7 \quad \\
10^3 & \equiv 8 \mod 7 \quad \\
10^4 & \equiv -1 \mod 7
\end{align*}
\]

Thus the number modulo 7 is the necessary choice of digit.

2. Show that for any list of odd primes \( \{p_1, \ldots, p_n\} \), there are \( n \) consecutive numbers with the \( i \)th number divisible by \( p_i \). For example, if the set was \( \{3, 5\} \) then the consecutive numbers 9, 10 work. Give a solution for the list \( \{29, 43, 7\} \).

3. Prove that if \( x \equiv a \mod n \) then either \( x \equiv a \mod 2n \) or \( x \equiv a + n \mod 2n \).

1) First we solve each congruence separately:

\[
\begin{align*}
5x & \equiv 3 \mod 9 \quad \iff 10x \equiv 6 \mod 9 \quad \iff x \equiv 6 \mod 9. \\
3x & \equiv 2 \mod 25 \quad \iff 3x \equiv 27 \mod 25 \quad \iff x \equiv 9 \mod 25. \\
14x & \equiv 17 \mod 43 \quad \iff 14x \equiv 60 \mod 43 \quad \iff 7x \equiv 30 \mod 43 \\
& \quad \iff 42x \equiv 180 \mod 43 \quad \iff x \equiv 18 \mod 43 \quad \iff x \equiv 15 \mod 43
\end{align*}
\]

Then we combine the three congruences to get 1 congruence mod 4325. So \( x \equiv -8 + 43r \equiv 9 \mod 25 \) implies \( 18r \equiv 17 \equiv 42 \mod 25 \) implies \( 3t \equiv 7 \mod 25 \) implies \( t \equiv -6 \mod 25 \). So \( x \equiv -8 + 43(-6 + 25u) \equiv 6 \mod 9 \), and therefore \( 1 - 2(3 - 2u) \equiv 6 \mod 9 \) which implies \( 4u \equiv 11 \equiv 2 \mod 9 \). So \( 2u \equiv 1 \mod 9 \) or \( u \equiv 5 \mod 9 \). Thus the solution is \( x \equiv -8 + 43(-6 + 25(5)) \mod 43259 \).

1) We are looking for a number \( m \) such that \( m \) is divisible by \( p_1 \), \( m + 1 \) is divisible by \( p_2 \), \( m + 2 \) is divisible by \( p_3 \) etc. In other words we want to solve the simultaneous congruences:

\[
m \equiv 0 \mod p_1, \quad m + 1 \equiv 0 \mod p_2, \ldots, m + (n - 1) \equiv 0 \mod p_n.
\]

The Chinese Remainder theorem guarantees that there exists a solution modulo \( p_1 \ldots p_n \). Any solution for \( m \) will have the property that \( m, m + 1 \ldots m + n - 1 \) are divisible by \( p_1, p_2 \ldots p_n \) respectively. To solve the particular problem involves another solutions to a Chinese Remainder problem:

\[
m \equiv 0 \mod 29, \quad m + 1 \equiv 0 \mod 43, \quad m + 2 \equiv 0 \mod 7.
\]

3) If \( x \equiv a \mod n \) then \( x = a + kn \) for some integer \( k \). \( k \) is either even or odd. If \( k \) is even then \( k = 2l \) for some integer \( l \) and thus \( x = a + 2ln \) and so \( x \equiv a \mod 2n \). If \( k \) is odd, \( k = 2l + 1 \) for some integer \( l \) and then \( x = a + (2l + 1)n = a + n + 2ln \) and so \( x \equiv a + n \mod 2n \).
1. Consider the following statement: "Given \( a \) not a multiple of \( p \), prove that \( a^m \equiv a^n \mod p \) if \( m \equiv n \mod f(p) \)."

   Give a function \( f \) so that the previous statement is true. Then prove the statement.

2. Compute the following expressions for any prime \( p \): \( 1^{p-1} + 2^{p-1} + \cdots + (p-1)^{p-1}, 1^p + 2^p + \cdots + (p-1)^p \).

3. Show that Mersenne numbers \( 2^p - 1 \) and Fermat numbers \( 2^{2^n} + 1 \) are either prime or pseudoprime.

   1) The function \( f(p) = p - 1 \) is what is desired since if \( m \equiv n \mod p - 1 \) then \( m = n + k(p - 1) \). Now if \( k \) is positive then \( a^m \equiv a^n a^{k(p - 1)} \equiv a^n (a^{p-1})^k \equiv a^n 1^k \mod p \) by Fermat’s little theorem. If \( k \) is negative then writing \( n = m - k(p - 1) \) we get \( a^n \equiv a^m (a^{p-1})^{-k} \equiv a^m 1^{-k} \equiv a^m \mod p \).

   2) Fermat’s little theorem tells us that the first expression is congruent to \( 1 + 1 + 1 + \cdots + 1 = p - 1 \mod p \) and the second expression is congruent to \( 1 + 2 + 3 + \cdots + p - 1 = \frac{p(p-1)}{2} \mod p \).