BBM 205 - Discrete Structures: Quiz 4 - Solutions
Date: 7.11.2018

Name:
Student ID:

1. (10 points) **Use the extended Euclid algorithm** to find integers x and y that satisfy

$$x \cdot 30 + y \cdot 22 = gcd(30, 22).$$

Solution:

$30 = 22 + 8$ $\quad rem(30, 22) = 8 = 30 - 22.$

$22 = 2 \cdot 8 + 6$ $\quad rem(22, 8) = 6 = 22 - 2 \cdot (30 - 22) = -2 \cdot 30 + 3 \cdot 22$

$8 = 6 + 2$ $\quad rem(8, 6) = 2 = 8 - 6 = (30 - 22) - (-2 \cdot 30 + 3 \cdot 22) = 3 \cdot 30 - 4 \cdot 22.$

$6 = 3 \cdot 2$ $\quad rem(6, 2) = 0.$

By this algorithm, $x = 3$ and $y = -4$ given in the question.

2. (10 points) Prove that $gcd(a^5, b^5) = (gcd(a, b))^5$ for every $a, b \in \mathbb{Z}$.

Solution:
The two claims below show that the statement is true.
Claim 1: $(gcd(a, b))^5 \leq gcd(a^5, b^5)$
Proof of Claim 1:
Let $k = gcd(a, b)$ such that $a = kx$ and $b = ky$. Since $a^5 = k^5x^5$ and $b^5 = k^5y^5$, we see that k^5 is a common divisor of both a^5 and b^5. Therefore, $k^5 | gcd(a^5, b^5)$, so the claim is true.

Claim 2: $(gcd(a, b))^5 \geq gcd(a^5, b^5)$
Proof of Claim 2: (by contradiction)
Again, let $k = gcd(a, b)$ such that $a = kx$ and $b = ky$. By the observation above, $k^5 | gcd(a^5, b^5)$. Assume that the negation of the claim is true, that is $(gcd(a, b))^5 = k^5 < gcd(a^5, b^5) = gcd(k^5x^5, k^5y^5)$. Since k^5 is a common divisor of a^5 and b^5, $gcd(a^5, b^5) = k^5 \cdot z$ for some integer $z > 1$. Let p be a prime divisor of z. Since p is prime and divides z, we have $p|x$ and $p|y$. However, this means $k \cdot p$ is a common divisor of a and b but greater that $gcd(a, b) = k$, a contradiction. The claim is true.

BBM 205 - Discrete Structures: Quiz 5 - Solutions
Date: 13.11.2018

Name:
Student ID:

Show all your work to receive full credit.

1. (5 points) What is the remainder of 63^{9601} divided by 220?

Solution: Note that $gcd(63, 220) = gcd(9 \cdot 7, 2^2 \cdot 5 \cdot 11) = 1$. Thus, by Euler's theorem,

$$63^{\Phi(220)} \equiv 1 \pmod{220}.$$

We can calculate $\Phi(220)$ by using the distinct prime divisors of 220 as $p_1 = 2$, $p_2 = 5$, $p_3 = 11$.

$$\Phi(220) = 220\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\left(1 - \frac{1}{p_3}\right) = 220\frac{1}{2} \cdot \frac{4}{5} \cdot \frac{10}{11} = 80.$$

So, $63^{80} \equiv 1 \pmod{220}$. Therefore,

$$63^{9601} \pmod{220} \equiv 63^1 \cdot (63^{80})^{120} \pmod{220} \equiv$$
$$\equiv 63^1 \cdot 1^{120} \pmod{220} \equiv 63 \pmod{220}.$$

2. (5 points) Simplify the following expression $3^{33} \pmod{11}$ using Fermat's Little Theorem.

Solution:

$$3^{33} \pmod{11} \equiv 3^3 \cdot (3^{10})^3 \pmod{11} \equiv 27 \cdot 1^3 \pmod{11} \equiv 5 \pmod{11}.$$

3. Bob would like to receive encrypted messages from Alice via RSA.

(a) (2 points) Bob chooses $p = 7$ and $q = 11$. His public key is (N, e). What is N?

Solution: $N = pq = 77$.

(b) (2 points) What number is e relatively prime to?

Solution: e must be relatively prime to $(p-1)(q-1) = 60$.

(c) (2 points) e need not be prime itself, but what is the smallest prime number e can be? Use this value for e in all subsequent computations.

Solution: We cannot take $e = 2, 3, 5$, so we take $e = 7$.

(d) (2 points) What is $\gcd(e, (p-1)(q-1))$?

Solution: By the RSA method's definition, $gcd(e, (p-1)(q-1)) = 1$.

(e) (2 points) What is the decryption exponent d? Do not calculate d, only describe what condition d should satisfy.

Solution: The decryption exponent is $d = e^{-1} \pmod{60}$

BBM 205 - Quiz 8

12.12.18

1. Show that the graph K_5 is not planar.

2. Draw the given planar graph without any crossings. How many faces are in your drawing?

Proof by Strong Induction Solutions

1. Determine which amounts of postage can be formed using just 3-cent and 10-cent stamps. Prove your answer by using strong induction.

   We will prove this statement using strong induction.
   Base case: We can form postage of 18, 19, and 20 cents using six 3-cent stamps, three 3-cent and one 10-cent stamp, and two 10-cent stamps.

   Inductive step: Our inductive hypothesis is that $P(j)$ is true for $18 \leq j \leq k$, where $k \in \mathcal{Z}$, $k \geq 20$. We want to show that $P(k+1)$ is true, which is to say we can form postage of $k+1$ cents.

   Using the inductive hypothesis, we assume $P(k-2)$ is true because $k-2 \geq 18$, and so we can form postage of $k-2$ cents using only 3-cent and 10-cent stamps. To form postage of $k+1$ cents, we need only add another 3-cent stamp to the stamps we used to form $k-2$ cents. Therefore, by strong mathematical induction, $P(k+1)$ is true whenever $P(k-2)$ is true. Q.E.D.

2. Use strong induction to show that every positive integer n can be written as the sum of distinct powers of two, that is, as a sum of a subset of integers $2^0 = 1$, $2^1 = 2$, $2^2 = 4$, and so on. Hint: For the inductive step, separately consider the case where $k+1$ is even and when it is odd. When it is even, note that $\frac{k+1}{2}$ is an integer.

   We will prove this statement using strong induction on n. Let n be a positive integer. We will prove that n can be written as the sum of distinct powers of 2. Let $P(n)$ be the statement that we can write n as the sum of distinct powers of 2.

   Base base: $P(1)$ is true because $1 = 2^0$.

   Inductive step: Assume for $1 \leq j \leq k$ for some integer k that $P(k)$ is true. That is, assume we can write all integers from 1 to k as the sum of distinct primes. We have two cases to consider.

   Case 1: k is even. Then, $k+1$ is odd. Now, by the inductive hypothesis, we have that k has an expansion

   $$k = 2^{m_1} + 2^{m_2} + \ldots + 2^{m_n}$$

   where $m_1 > m_2 > \ldots > m_n$. (Note: we need to write it in general terms because we don't know which powers of 2 are needed for the integer. There is no reason that k would have to have 2 or 4 or any other particular power of 2 in it's expansion.). Notice that since k is even, there is no 2^0 in the expansion; so, from the expansion for k we add 2^0 to yield

   $$k = 2^{m_1} + 2^{m_2} + \ldots + 2^{m_n} + 2^0$$

to give the expansion for k_1.

Case 2: k is odd. Then $k+1$ is even. (Note: we can't do the same as the other case because we already have a 2^0 in the expansion of k and so a second one would mean we would have to change it to 2^1 to make it unique, but then if we already have a 2^1 in the expansion, we have to change that to a 2^2, which we may already have, and since we don't actually see the expansion for a generic k, we can't begin to approach this way). Since $k+1$ is even, then $\frac{k+1}{2} \in \mathcal{Z}$ and therefore by the inductive hypothesis, has an expansion consisting of the sum of distinct powers of 2. Let the expansion be

$$\frac{k+1}{2} = 2^{m_1} + 2^{m_2} + \ldots + 2^{m_n}$$

Then, we can multiply both sides by 2, yielding

$$2\left(\frac{k+1}{2}\right) = 2(2^{m_1} + 2^{m_2} + \ldots + 2^{m_n})$$
$$k+1 = 2^{m_1+1} + 2^{m_2+1} + \ldots + 2^{m_n+1}$$

which completes the inductive step. So, by strong induction, we have shown that if $P(j)$ is true for $1 \leq j \leq k$, then $P(k+1)$ is true as well. Q.E.D.