CONCORDIA UNIVERSITY DEPARTMENT OF COMPUTER SCIENCE AND SOFTWARE ENGINEERING

COMP 239/4 Mathematics for Computer Science II WINTER 2005

Assignment 1 solution

1. Let n be a positive integer. Prove that if $2^n + 1$ is a prime number greater than 3, then n is even.

   Solution. We will prove the contrapositive. If n is a positive odd integer, then

   $$2^n + 1 \equiv (-1)^n + 1 \equiv -1 + 1 \equiv 0 \pmod 3$$

   and so 3 divides $2^n + 1$. It follows that either $2^n + 1 \leq 3$ or else $2^n + 1$ is composite.

2. Prove that for any natural numbers a and b the number

   $$\gcd(a + b, ab) - \gcd(a, b)$$

   is even.

   Solution. The proof is by cases. First assume that both a and b are even. Then $a+b$ and ab are even so $\gcd(a+b, ab)$ and $\gcd(a, b)$ are even and thus $\gcd(a+b, ab) - \gcd(a, b)$ is even. Next assume that both numbers are odd. Then $a+b$ is even and ab is odd. So $\gcd(a+b, ab)$ and $\gcd(a, b)$ are odd and again $\gcd(a+b, ab) - \gcd(a, b)$ is even. Finally assume that a and b have different parities. Then $a + b$ is odd and ab is even. So $\gcd(a + b, ab)$ and $\gcd(a, b)$ are odd and again $\gcd(a + b, ab) - \gcd(a, b)$ is even.

3. Determine the last two digits of the number

   $$2^{5^1} + 2^{5^2} + \ldots + 2^{5^{1991}}.$$

   (Hint: Use induction on k to evaluate 2^{5^k} modulo 100.)

   Solution. We first prove by induction that

   $$2^{5^k} \equiv 32 \pmod{100}$$

   for all positive integers k. Indeed for $k = 1$ we have $2^5 = 32 \equiv 32 \pmod{100}$. Assuming that the congruence holds for some positive integer k we have

   $$2^{5^{k+1}} = (2^{5^k})^5 \equiv 32^5 = (30 + 2)^5 \equiv 2^5 = 32 \pmod{100}.$$

   Hence

   $$2^{5^1} + 2^{5^2} + \ldots + 2^{5^{1991}} \equiv 1991 \cdot 32 \equiv 91 \cdot 32 = 2912 \equiv 12 \pmod{100}$$

   thus the last two digits of the sum are 12.

4. (a) Write the binary expansion of 19.

   (b) Let k be the number of digits in this binary expansion. Compute the powers

   $$13 \bmod 151, 13^2 \bmod 151, 13^{2^2} \bmod 151, \ldots, 13^{2^{k-1}} \bmod 151.$$

   (c) Use the previous two questions to compute $13^{19} \bmod 151$.

   Solution.

   (a) We have $19 = 1 + 2 + 2^4$ so $(10011)_2$ is the binary expansion of 19.

   (b) The number of digits in the binary expansion of 13 is 5. We compute $13 \bmod 151 = 13$, $13^2 \bmod 151 = 18$, $13^{2^2} \bmod 151 = 22$, $13^{2^3} \bmod 151 = 31$ and $13^{2^4} \bmod 151 = 55$. (Note that each power is obtained by squaring the previous one and taking the remainder modulo 151.)

   (c) By (a) we know that $13^{19} = 13^{1+2+2^4} = 13 \times 13^2 \times 13^{2^4}$ and by (b) we get that $13^{19} \equiv 13 \times 18 \times 55 \equiv 12870 \pmod{151}$ so $13^{19} \bmod 151 = 12870 \bmod 151 = 35$.

5. Let n be a positive integer.

   (a) Prove that n is divisible by 2 if and only if it ends with $0, 2, 4, 6$ or 8.

   (b) Prove that n is divisible by 3 if and only if the sum of its digits is divisible by 3.

   (c) Prove that n is divisible by 5 if and only if it ends with 0 or 5.

   (d) Prove that n is divisible by 9 if and only if the sum of its digits is divisible by 9.

   (e) Find a similar criterion for divisibility by 11 and prove it.

   Solution. Note that n is divisible by p if and only if $n \equiv 0 \pmod{p}$. Let $d_0, d_2, \ldots, d_k$ be the digits of n (starting from the left). Then $n = 10^k d_0 + 10^{k-1} d_1 + \cdots + 10 d_{k-1} + d_k$.

   (a) Since $10 \equiv 0 \pmod 2$, we have $n \equiv d_k \pmod 2$, so n is divisible by 2 if and only if $2 \mid d_k$, that is if and only if d_k is 0, 2, 4, 6 or 8.

   (b) Since $10 \equiv 1 \pmod 3$, we have $n \equiv d_0 + d_1 + \cdots + d_{k-1} + d_k \pmod 3$ so n is divisible by 3 if and only if the sum of the digits of n, that is $d_0 + d_1 + \cdots + d_k$, is divisible by 3.

   (c) This case is similar to the first case since $10 \equiv 0 \pmod 5$. So n is divisible by 5 if and only if d_k is divisible by 5, that is d_k is 0 or 5.

   (d) This case is similar to the second case since $10 \equiv 1 \pmod 9$. So n is divisible by 9 if and only if the sum of its digits is divisible by 9.

   (e) We have $10 \equiv -1 \pmod{11}$ so $n \equiv (-1)^k d_0 + (-1)^{k-1} d_1 + \cdots - d_{k-1} + d_k \pmod{11}$. Therefore n is divisible by 11 if and only the sum of its digits counted alternately as positive or negative is divisible by 11.

6. Compute two integers s and t such that

$$666s + 1414t = 2.$$

Solution. The GCD of 666 and 1414 is 2, so we can use an extended Euclidean algorithm to find two integers s and t such that

$$1414s + 666t = 2.$$

Here is the trace of the algorithm (refer to the handout The Extended Euclid Algorithm on the course web page for explanation of notation):

n	q	r	s	t
0		1414	1	0
1		666	0	1
2	2	82	1	−2
3	8	10	−8	17
4	8	2	65	−138
5	5	0	−333	707

Hence we get $s = 65$ and $t = -138$.

7. Show that the system of congruences

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \end{aligned}$$

has solution if and only if $\gcd(m_1, m_2)|(a_1 - a_2)$. Show that when there is a solution, it is unique modulo $\text{lcm}(m_1, m_2)$.

Solution. Let $\gcd(m_1, m_2) = (m_1, m_2)$ and $\text{lcm}(m_1, m_2) = [m_1, m_2]$. The system of congruences implies that $x = a_1 + km_1$ and $x = a_2 + jm_2$, where k and j are some integers. Hence $a_1 + km_1 = a_2 + jm_2$ or $jm_2 - km_1 = a_1 - a_2$. Thus $a_1 - a_2 = (m_1, m_2)(jm_2/(m_1, m_2) - km_1/(m_1, m_2))$ because (m_1, m_2) divides m_1 and m_2. So there is a solution only if $(m_1, m_2)|(a_1 - a_2)$.
Now suppose that $(m_1, m_2)|(a_1 - a_2)$. Since (m_1, m_2) can be written as a linear combination of m_1 and m_2 with integer coefficients, $a_1 - a_2$ can be written as linear combination of m_1 and m_2, say $jm_2 - km_1 = a_1 - a_2$, for some integers j and k, or $a_1 + km_1 = a_2 + jm_2$. Then $x = a_1 + km_1$ is a solution to $x \equiv a_1 \pmod{m_1}$, and $x = a_1 + km_1 = a_2 + jm_2 \equiv a_2 \pmod{m_2}$. Thus $x = a_1 + km_1 + l[m_1, m_2] = a_2 + jm_2 + l[m_1, m_2]$ is a solution of the original system of congruences for any integer l since $x = a_1 + km_1 + l[m_1, m_2] \equiv a_1 \pmod{m_1}$ and $x = a_1 + km_1 + l[m_1, m_2] = a_2 + jm_2 + l[m_1, m_2] \equiv a_2 \pmod{m_2}$.

To prove uniqueness assume that x_1 and x_2 are two solutions of the system of congruences. Thus

$$\begin{aligned} x_1 &\equiv a_1 \pmod{m_1} \\ x_1 &\equiv a_2 \pmod{m_2} \end{aligned}$$

and

$$\begin{aligned} x_2 &\equiv a_1 \pmod{m_1} \\ x_2 &\equiv a_2 \pmod{m_2}. \end{aligned}$$

Hence

$$\begin{aligned} x_1 &\equiv x_2 \pmod{m_1} \\ x_1 &\equiv x_2 \pmod{m_2} \end{aligned}$$

which implies $x_1 \equiv x_2 \pmod{[m_1, m_2]}$.

8. Find all solutions of the following systems of linear congruences.

(a)

$$\begin{aligned} x &\equiv 2 \pmod 3 \\ x &\equiv 2 \pmod 5 \\ x &\equiv 0 \pmod 4 \end{aligned}$$

(b)

$$\begin{aligned} x &\equiv 10 \pmod{60} \\ x &\equiv 80 \pmod{350} \end{aligned}$$

Solution.

(a) $N_1 = 20$, $x_1 = 2$, $N_2 = 12$, $x_2 = 3$, $N_3 = 15$, $x_3 = 3$, where $N_1 x_1 \equiv 1 \pmod 3$, $N_2 x_2 \equiv 1 \pmod 5$ and $N_3 x_3 \equiv 1 \pmod 4$. Hence the solution is $x = 2 \cdot 20 \cdot 2 + 2 \cdot 12 \cdot 3 + 0 \cdot 15 \cdot 3 \equiv 32 \pmod{60}$.

7. 2 (b) Since gcd(60, 350) divides 10-80, our solution of Exercise 7 specializes as follows. Using the extended Euclidean algorithm, we find that gcd(60, 350) = 10 = 6*60+(−1)*350. It follows that 10-80 = 7*350 - 42*60, which can be written as 10 + 42*60 = 80 + 7*350. Since 10 + 42*60 = 2530 and lcm(60, 350) = 2100, we conclude that all solutions of our system of congruences are precisely all solutions of the single congruence

$$x \equiv 2530 \equiv 430 \pmod{2100}.$$

9. Decode the message

1684 2311 1943 1723 2268 2417

using the RSA coding system with $p = 43$, $q = 59$, and $e = 13$. (Hint: use the method described in Question 4 to perform exponentiations.)

Solution. An inverse of e modulo $(p-1)(q-1) = 2436$ is 937 and $1684^{937} \bmod pq = 0308$, $2311^{937} \bmod pq = 1802$, $1943^{937} \bmod pq = 1704$, $1723^{937} \bmod pq = 1904$, $2268^{937} \bmod pq = 1200$ and $2417^{937} \bmod pq = 1907$. When each four-digit integer is interpreted as two two-digit integers, the solution 308 1802 1704 1904 1200 1907 is interpreted as 3 8 18 2 17 4 19 4 12 0 19 7. Then the substitution of A for 0, B for 1, ..., Z for 25 yields the message DISCRETEMATH.

CONCORDIA UNIVERSITY DEPARTMENT OF COMPUTER SCIENCE

COMP 239 Mathematics for Computer Science II FALL 1999

Mid-term Test 2

Time allowed: 1 hr 10 mins.

It is morally and ethically wrong to cheat, plagiarize, or copy from others. The penalties can be severe.

Instructions:

i) Do all questions.

ii) No calculators, notes, crib sheets are permitted.

iii) No marks will be given to answers without details of your calculations.

Questions:

1. How many solutions are there to the equation $x_1 + x_2 + x_3 = 17$, where x_1, x_2, x_3 are non-negative integers with

   a) $x_1 > 1$, $x_2 > 2$, $x_3 > 3$?

   b) $x_1 < 6$, $x_3 > 5$.

   c) $x_1 < 4$, $x_2 < 3$, $x_3 > 5$.

2. Find f(n) when $n = 3^k$, where f(n) satisfies the recurrence relation

$$f(n) = 2f(n/3) + 4 \text{ with } f(1) = 1.$$

3. Solve the linear nonhomogeneous recurrence relation: $a_n = 2a_{n-1} + 5^n$, for $a_0 = 1$ and $n \geq 0$.

4. Show that:

$$a_n = \frac{17 - \sqrt{17}}{34}\left(\frac{3 + \sqrt{17}}{2}\right)^n + \frac{17 + \sqrt{17}}{34}\left(\frac{3 - \sqrt{17}}{2}\right)^n$$

   is an integer for all $n \geq 0$.

   Hint: a_n has the form of $C_1 r_1^n + C_2 r_2^n$.

5. Find the recurrence relation for the number of strings of n decimal digits containing an even number of zeros. What are the initial conditions?

COMP 239
Solutions to Mid-Term Test 2

1. a) $x_1 \geq 2, x_2 \geq 3, x_3 \geq 4 \Rightarrow C(8+3-1,8) = C(10,8) = \underline{45}$.

   b) Condition $x_3 \geq 6$ gives: $x_3 = x_3' + 6$

   or $x_1 + x_2 + x_3' = 11 \Rightarrow C(13,11) = 78$

   Condition $x_1 < 6$ then gives (remove all solutions with $x_1 \geq 6$):

   N = 78 − C(5+3-1,5) = 78 − C(7,5) = $\underline{57}$.

   c) Condition $x_3 \geq 6$ gives: $x_3 = x_3' + 6$

   or $x_1 + x_2 + x_3' = 11 \Rightarrow C(13,11) = 78$.

   Now, we have to remove the solutions with $x_1 \geq 4$ and $x_2 \geq 3$:

   N = 78 − C(7+3-1,7) − C(8+3-1,8) + C(4+3−1,4)
   = 78 − 36 − 45 + 15
   = $\underline{12}$

2.
$$\begin{aligned} f(n) &= 2f(\tfrac{n}{3}) + 4 \quad \text{Assume } n = 3^k \\ &= 2\left[2f(\tfrac{n}{3^2}) + 4\right] + 4 \\ &= 2^2 f(\tfrac{n}{3^2}) + 2.4 + 4 \\ &= 2^3 f(\tfrac{n}{3^3}) + 2^2.4 + 2^1.4 + 2^0.4 \\ &= 2^k f(\tfrac{n}{3^k}) + (2^{k-1} + 2^{k-2} + \cdots + 2^0)4 \\ &= 2^k + (2^k - 1)4 \\ &= 5.2^k - 4 \\ &= 5n^{\log_3 2} - 4. \end{aligned}$$

3. Homogeneous solution: $a_n - 2a_{n-1} = 0 \Rightarrow r = 2 \Rightarrow a_n^{(h)} = C.2^n$

   Trial solution: $a_n^{(p)} = \alpha 5^n \Rightarrow \alpha 5^n = 2\alpha.5^{n-1} + 5^n$ or $\alpha = \frac{5}{3}$.

   Therefore, $a_n = C2^n + \frac{5}{3}5^n$ with $a_0 = 1 = C + \frac{5}{3}$

   or $C = \frac{-2}{3}$. Hence: $a_n = \frac{1}{3}\left[5^{n+1} - 2^{n+1}\right]$.

4. a_n has the form $c_1 r_1^n + c_2 r_2^n$ where r_1, r_2 are two roots of a quadratic equation (characteristic equation of a linear recurrence). For a quadratic equation $ar^2 + br + c = 0$, the roots are: $\frac{-b \pm \sqrt{b^2-4ac}}{2a}$.

   Compare these roots with r_1, r_2 in a_n, we have:

   b = −3, a = 1, and c = −2. Therefore the characteristic equation is $r^2 - 3r - 2 = 0$ or