Math 1580 Midterm Exam 2011

Name: _____

- The exam will last 50 minutes.
- There are 5 problems worth 12 points each.
- No notes or other study materials allowed.
- Any calculators must be limited to basic arithmetic operations only. No scientific calculators or smartphones.
- Use the backside of the test pages for scratch work, or if you need extra space.

1	
2	
3	
4	
5	
Total	

Problem 1. This question has 3 parts.

(a) Give a description of the Miller-Rabin algorithm for testing the primality of a given number n.

(b) Suppose that the test fails for 10 randomly selected elements a. What is the approximate probability that n is prime?

(c) Suppose you find that $858^2 \equiv 1 \pmod{736163}$. What can you conclude about the number 736163?

Solution. (a) Let $n-1 = 2^k q$, with q odd, and choose a randomly selected input a such that $1 \leq a \leq n-1$.

(1) Set $a_0 = a^q \pmod{n}$.

(2) If $a_0 \equiv 1 \pmod{n}$, then return **fail** (n might possibly be prime.)

(3) Loop over $i = 0, 1, \ldots, k-1$:

(4) If $a_i \equiv -1 \pmod{n}$, then return **fail**, otherwise set $a_{i+1} \equiv a_i^2 \pmod{n}$ and continue looping.

(5) If the loop finishes, return **composite.**

(b) The probability that the algorithm fails given that n is composite is at most $1/4$. Therefore if the test fails 10 times, the probability that n is composite is approximately 4^{-10}, and therefore the probability that n is prime is approximately

$$1 - 4^{-10}.$$

(c) 736163 cannot be prime, otherwise the only solutions to $x^2 \equiv 1 \pmod{736163}$ would be 1 and -1. In fact, (though you were not required to do this),

$$858^2 - 1 \equiv 0 \pmod{736163} \implies (858-1)(858+1) = (857)(859) = k(736163)$$

for some k, and upon inspection, $k = 1$.

□

Problem 2. Alice and Bob are using the ElGamal cryptosystem to exchange messages, with prime $p = 71$ and primitive root $g = 62$. Alice chooses secret key $a = 2$, and computes her public key $A = g^a \equiv 10 \pmod{71}$. Bob sends her the ciphertext

$$(c_1, c_2) = (g^b, A^b\, m) = (9, 1).$$

What is Bob's message?

Solution. Alice needs to compute

$$m = A^{-b}c_2 = g^{-ab}c_2 = \left(g^b\right)^{-a} c_2 = c_1^{-a}c_2 \pmod{p}.$$

We compute

$$c_1^a = 9^2 = 81 \equiv 10 \pmod{71}$$

and from long division,

$$71 = 7 \cdot 10 + 1 \implies -7 \cdot 10 \equiv 1 \pmod{71} \implies 10^{-1} \equiv -7 \equiv 64 \pmod{71}$$

Finally,

$$m = 9^{-2} \cdot 1 \equiv 10^{-1} \cdot 1 \equiv 64 \cdot 1 \equiv 64 \pmod{71}. \qquad \square$$

Problem 3. Compute

$$5597^{1018^{406}} \pmod{11}.$$

Solution. The easiest way is to use

$$\begin{aligned} 5597^{1018^{406}} \pmod{11} &= (5597 \pmod{11})^{\left(1018^{406} \pmod{\phi(11)}\right)} \\ &= (5597 \pmod{11})^{(1018 \pmod{10})^{406} \pmod{\phi(10)}} \end{aligned}$$

and since $\phi(10) = \phi(2)\phi(5) = 4$ and $406 \pmod 4 = 2$, we compute

$$1018^{406} \pmod{10} \equiv 8^2 \pmod{10} = 4.$$

Finally, $5597 = 5599 - 2 = 11 \cdot 509 - 2 \equiv -2 \equiv 9 \pmod{11}$ so

$$5597^{1018^{406}} \pmod{11} = 9^4 \pmod{11} \equiv 81^2 \pmod{11} \equiv (-7)^2 \pmod{11} \equiv 49 \pmod{11} = 5.$$

Alternatively, you could use fast powering to compute $1018^{406} \pmod{10}$:

$$406 = 256 + 128 + 16 + 4 + 2 = 2^8 + 2^7 + 2^4 + 2^2 + 2^1$$

and computing successive squares mod 10,

i	0	1	2	3	4	5	6	7	8
$8^{2^i} \pmod{10}$	8	4	6	6	6	6	6	6	6

Thus

$$1018^{406} \pmod{10} \equiv 8^{2^8}8^{2^7}8^{2^4}8^{2^2}8^{2^1} \equiv 6 \cdot 6 \cdot 6 \cdot 6 \cdot 4 \equiv 4 \pmod{10}.$$

The computation of $5597^{1018^{406}} \pmod{11}$ is now the same. □

Problem 4. You already proved on a homework problem that for p an odd prime, the congruence $x^2 \equiv a \pmod{p}$ either has no solutions, or it has two solutions.

(a) Let $n = pq$ be the product of distinct odd primes. Show that if $x^2 \equiv a \pmod{n}$ has a solution, then it has exactly four solutions.

(b) Suppose you had access to a machine that could tell you all four solutions. How could you use this information to factor n?

Solution. (a) Let x_0 be a solution to $x^2 \equiv a \pmod{n}$. It follows that the equations

$$x^2 \equiv a \pmod{p} \quad \text{and} \quad x^2 \equiv a \pmod{q}$$

each have two solutions since $x_0 \pmod{p}$ and $x_0 \pmod{q}$ are solutions.

Let b_1, b_2 be the solutions to $x^2 \equiv a \pmod{p}$ and c_1, c_2 be the solutions to $x^2 \equiv a \pmod{q}$. By the Chinese Remainder Theorem, each of the simultaneous congruences

$$x \equiv b_i \pmod{p}, \quad x \equiv c_j \pmod{q}, \quad i, j \in \{1, 2\}$$

has a unique solution modulo n, and these must be distinct. Since there are four possibilities for (i, j), this gives 4 distinct solutions to the original equation.

(b) By assumption we would have 4 distinct numbers $d_i : i = 1, \ldots, 4$ which satisify $d_i^2 \equiv a \pmod{n}$. Thus for any pair with $i \neq j$,

$$d_i^2 - d_j^2 \equiv 0 \pmod{n} \implies n | (d_i - d_j)(d_i + d_j)$$

and whenever we have this situation we can hope that $\gcd(d_i - d_j, n)$ is a nontrivial factor of n.

In fact $d_i - d_j$ will split n precisely when $d_i \equiv d_j \pmod{p}$ but $d_i \not\equiv d_j \pmod{q}$ or vice versa.

□

Problem 5. This question has 2 parts.

(a) Prove that if $f(x) = \mathcal{O}\big(g(x)\big)$ and $g(x) = \mathcal{O}\big(h(x)\big)$, then $f(x) = \mathcal{O}\big(h(x)\big)$.

(b) If $f(x) \neq \mathcal{O}\big(g(x)\big)$, then must it be true that $g(x) = \mathcal{O}\big(f(x)\big)$? Justify your answer by giving a proof or a counterexample.

Solution. (a) By assumption, there exist C_1, c_1, C_2, c_2 such that

$$x \geq C_1 \implies f(x) \leq c_1 g(x) \quad \text{and} \quad x \geq C_2 \implies g(x) \leq c_2 h(x).$$

Setting $C = \max C_1, C_2$ and $c = c_1 c_2$ it follows that

$$x \geq C \implies f(x) \leq c_1 g(x) \leq c_1 c_2 h(x) = c h(x)$$

and therefore $f(x) = \mathcal{O}\big(h(x)\big)$.

(b) No. For instance

$$\sin(x) \neq \mathcal{O}\big(\cos(x)\big) \quad \text{and} \quad \cos(x) \neq \mathcal{O}\big(\sin(x)\big).$$

□