MATH 3094 - Second Practice Midterm

YOUR NAME: ÁLVARO

P1	P2	P3	P4	P5	Extra	Total

Show all your work. Explain all your answers. Do not use calculator programs.

Problem 1. (25 points) For each problem below, **explain** your steps to find the answer.

(1) *Understand the meaning and how to compute with Legendre symbols.* Find the values of

$$\left(\frac{2}{29}\right), \left(\frac{-1}{29}\right), \left(\frac{17}{29}\right), \left(\frac{29}{17}\right).$$

$\left(\frac{2}{29}\right) = (-1)^{\frac{29^2-1}{8}} = -1$

$\left(\frac{-1}{29}\right) = (-1)^{\frac{29-1}{2}} = 1$

$12 = 3 \cdot 4$

$\left(\frac{17}{29}\right) \overset{QR}{=} \left(\frac{29}{17}\right) = \left(\frac{12}{17}\right) = \left(\frac{3}{17}\right) = \left(\frac{17}{3}\right) = \left(\frac{2}{3}\right) = -1.$

$QR + 17 \equiv 1 \bmod 4$

$\left(\frac{29}{17}\right) = \left(\frac{17}{29}\right) = -1$

(2) *Find primes satisfying certain congruence conditions and/or certain Legendre conditions.* Find primes p and q such that $p = 2q + 1$. Both p and q should be > 15.

Let $q = 23$, $p = 2 \cdot 23 + 1 = 47$.

Then p and q are primes s.t. $2q+1 = p$.

$q = 23$

$p = 47$

(3) Find three distinct primes p such that $\left(\frac{p}{7}\right) = 1$.

$QR's = \{1, 2, 4\}$

$QNR's = \{3, 5, 6\}$

If $\left(\frac{p}{7}\right) = 1$ then $p \equiv$ QR $\bmod 7$.

$\Rightarrow p \equiv 1, 2,$ or $4 \bmod 7$

$\Rightarrow p = 2, 11, 23$ work!

(4) *Learn how to use the law of quadratic reciprocity.* Compute $\left(\frac{19}{41}\right)$ using Gauss's Law of Quadratic Reciprocity.

$\left(\frac{19}{41}\right) \overset{QR}{=} \left(\frac{41}{19}\right) = \left(\frac{3}{19}\right) = -\left(\frac{19}{3}\right) = -\left(\frac{1}{3}\right) = (-1) \cdot 1 = -1$

$41 \equiv 1 \bmod 4$

$41 \equiv 3 \bmod 19$

$19 \equiv 3 \bmod 4$

Problem 2. (25 points) Let $N = 221$.

(1) *Learn how to use the Fermat primality test.* Is 2 a Fermat witness for the compositeness of N?

We find $2^{220} \bmod 221$: $220 = 128 + 64 + 16 + 8 + 4$

$2, 4, 8, 64, 4096 \equiv 118 \bmod 221$

$2^8 \equiv 256 \equiv 35$, $2^{16} \equiv 35^2 \equiv 1225 \equiv 120$, $2^{32} \equiv 120^2 \equiv 35$

$2^{64} \equiv 120$, $2^{128} \equiv 35$

Thus, $2^{220} \equiv 2^{128} \cdot 2^{64} \cdot 2^{16} \cdot 2^8 \cdot 2^4 \equiv 16 \bmod 221$

Thus 2 is a witness and 221 is NOT prime!

(2) *Learn how to use the Miller–Rabin primality test.* Is 2 a Miller–Rabin witness for the compositeness of N?

$220 = 2^2 \cdot 55$. Let $q = 55$.

$2^{55} \equiv 128 \neq 1, -1 \bmod 221$

$2^{110} \equiv 30 \neq -1 \bmod 221$

} Yes, 2 is a M-R witness!

221 is NOT prime.

(3) *Learn how to use Pollard's $p-1$ method to find a factorization of N.* Use Pollard's $p-1$ method to find a factorization of N. Please indicate clearly each step of the algorithm.

Let $a = 2$.

- $a^2 = 2^2 = 4$, $\gcd(3, N) = 1$ ← 4−1
- $a^6 = 4^3 = 64$, $\gcd(63, N) = 1$
- $a^{24} = 64^4 \equiv 1 \bmod 221$, $\gcd(0, N) = N$
- $a^{5!} \equiv 1 \bmod 221$, $\gcd(0, 221) = 1$
- $a^{21!}$ ... STOP, use another value!

$a = 3$

- $a^2 \equiv 9$, $\gcd(8, N) = 1$
- $a^6 \equiv 9^3 \equiv 66$, $\gcd(65, N) = 13$

$\Rightarrow 13 \mid N$

$\boxed{N = 13 \cdot 17}$

Problem 3. (25 points) *Learn how to use RSA.* In this problem, $N = 221$, as in Problem 2. Alice wants to set up an RSA encryption scheme with N as her modulus.

(1) Can Alice choose e = 3 as an encryption exponent?

$N = 221 = 13 \cdot 17$

$\varphi(N) = 12 \cdot 16 = 2^6 \cdot 3$

e needs to be rel. prime to $\varphi(N)$

so NO, cannot use $e = 3$.

(2) Can Alice choose $e = 7$ as an encryption exponent?

Yes, because $\gcd(7, \varphi(N)) = 1$.

(3) If $e = 7$, what is the decryption exponent d?

We need d s.t. $7d \equiv 1 \mod \varphi(N) = 192$.

$\Rightarrow \boxed{d = 55}$

(Euclid's or otherwise)

(4) Alice sets up RSA with $(N, e) = (221, 7)$. Bob wants to send the message $m \equiv 2 \mod 221$. What is the encrypted message? How does Alice decrypt the message?

Cipher: $m^e \mod 221$, so $2^7 \equiv 128 \mod 221$

Alice decrypts:

$m \equiv c^d \equiv 128^{55} \equiv 2 \mod 221$.

(5) Alice sets up RSA with $(N, e) = (323, 5)$ and Eve intercepts a message from Bob with cipher 11 mod 323. What was Bob's original message?

Since $N = 323 = 17 \cdot 19$ and $\varphi(N) = 288$

we find $d = 173$ so

$m \equiv 11^{173} \equiv 7 \mod 323$

(note $7^5 \equiv 11 \mod 323$)

Problem 4. (25 points) *Learn how to use the Primer Number Theorem, and the confidence probabilities associated to Miller Rabin tests.*

(1) Consider the number $n = 300001$. According to the prime number theorem, how likely is it that n is a prime number?

About $\frac{1}{\log n} = \frac{1}{\log(300001)} = 0.0792924\ldots$

or $7.92924\ldots\%$

(NOTE: It is NOT prime)

(2) Approximately, how many primes are there in the interval $[300000, 400000]$ according to the prime number theorem?

There are about

$\pi(400000) - \pi(300000)$ primes or

$\frac{400000}{\ln(400000)} - \frac{300000}{\ln(300000)} = 7221.88\ldots$ primes.

(3) If a is an integer that is *not* Miller Rabin witness for the compositeness a number p, what is the probability that p is prime? What if we found two integers a and b that are *not* Miller Rabin witnesses for p, what is the probability that p is prime?

at least 75% of numbers are witnesses for p (composite)

at most 25% are not witnesses

$\Rightarrow$ 25% chance it's composite or $\frac{1}{4}$. $\Rightarrow$ 75% it's prime

$P(\text{a is NOT witness}) \cdot P(\text{b is NOT witness}) = \frac{1}{4} \cdot \frac{1}{4} = \frac{1}{16}$ or 6.25% it's composite

or 93.75% it's prime.

Problem 5. (25 points) *Learn how to use the digital signature algorithms we saw in class: RSA, Elgamal, and DSA.*

(1) Sam sets up an RSA digital signature protocol with $N = 221$. Sam chooses $e = 7$, and the document to be signed is $D \equiv 10 \bmod 221$. Produce a signature for D.

$N = 221$, $\varphi(N) = 192$, $e = 7 \Rightarrow d = 55$

$D \equiv 10$ $S \equiv 10^{55} \equiv 192 \bmod 221 \Rightarrow (D, S) = (10, 192)$

(2) Help Victor verify that the signature in part (1) is legitimate.

$S^e \equiv 192^7 \equiv 10 \equiv D \bmod 221$ ✓

(3) Sam sets up an Elgamal digital signature protocol with $p = 43$ and $g = 3$. Sam chooses $a = 5$, $k = 2$, and the document to be signed is $D \equiv 10 \bmod 43$. Produce a signature for D.

$A \equiv g^a \equiv 3^5 \equiv 28 \bmod 43$

$D \equiv 10 \Rightarrow S_1 \equiv 3^2 \equiv 9 \bmod 43$

$S_2 \equiv (10 - 5 \cdot 9) \cdot 2^{-1} \bmod 42$ } CAN'T! k is invalid! $\gcd(k, p-1) \neq 1$.

(4) Help Victor verify that the signature in part (3) is legitimate.

k was invalid and a signature was not produced.

(5) Sam sets up a DSA digital signature protocol with $p = 43$, $q = 7$, and $g = 41$. Sam chooses $a = 5$, $k = 2$, and the document to be signed is $D \equiv 10 \bmod 43$. Produce a signature for D.

~~$m \equiv k \bmod 43$~~, $D \equiv 10$, $A \equiv g^a \equiv 41^5 \equiv 11 \bmod 43$

$S_1 \equiv (41^2 \bmod 43) \bmod 7 \equiv 4$

$S_2 \equiv (D + a S_1) k^{-1} \bmod q \equiv (10 + 5 \cdot 4) \cdot 2^{-1} \bmod 7 \equiv 15 \equiv 1 \bmod 7$ } $(D, S_1, S_2) = (10, 4, 1)$

(6) Help Victor verify that the signature in part (5) is legitimate.

$V_1 \equiv 10 \cdot 1^{-1} \equiv 10 \equiv 3 \bmod 7$

$V_2 \equiv 4 \cdot 1^{-1} \equiv 4 \bmod 7$

$(41^3 \cdot 11^4 \equiv 44 \bmod 43) \equiv 4 \bmod 7 \equiv S_1$ ✓