

MATH 3094 - Second Practice Midterm

YOUR NAME: ALVARO

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

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

$\left(\frac{2}{29}\right) = (-1)^{\frac{29^2-1}{8}} = -1$
 $\left(\frac{-1}{29}\right) = (-1)^{\frac{29-1}{2}} = 1$
 $\left(\frac{17}{29}\right) \stackrel{QR}{=} \left(\frac{29}{17}\right) = \left(\frac{12}{17}\right) = \left(\frac{3}{17}\right) = \left(\frac{17}{3}\right) = \left(\frac{2}{3}\right) = -1.$
 $\left(\frac{29}{17}\right) = \left(\frac{17}{29}\right) = -1$

$12 = 3 \cdot 4$
 $QR + 17 \equiv 1 \pmod{4}$

- (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. $2q + 1 = p$.

$\begin{matrix} q=23 \\ p=47 \end{matrix}$

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

If $\left(\frac{p}{7}\right) = 1$ then $p \equiv \text{QR} \pmod{7}$. QR's = $\{1, 2, 4\}$
 QNR's = $\{3, 5, 6\}$

$\Rightarrow$ ~~$p = 3, 5, 6, 11, 13, 17, 19, 23, 25, 29, 31, 35, 37, 41, 43, 47, 53, 55, 59, 61, 65, 67, 71, 73, 75, 79, 83, 85, 89, 91, 95, 97, 101, 103, 105, 109, 111, 113, 115, 119, 121, 123, 125, 129, 131, 133, 135, 139, 141, 143, 145, 149, 151, 153, 155, 159, 161, 163, 165, 169, 171, 173, 175, 179, 181, 183, 185, 189, 191, 193, 195, 199, 201, 203, 205, 209, 211, 213, 215, 219, 221, 223, 225, 229, 231, 233, 235, 239, 241, 243, 245, 249, 251, 253, 255, 259, 261, 263, 265, 269, 271, 273, 275, 279, 281, 283, 285, 289, 291, 293, 295, 299, 301, 303, 305, 309, 311, 313, 315, 319, 321, 323, 325, 329, 331, 333, 335, 339, 341, 343, 345, 349, 351, 353, 355, 359, 361, 363, 365, 369, 371, 373, 375, 379, 381, 383, 385, 389, 391, 393, 395, 399, 401, 403, 405, 409, 411, 413, 415, 419, 421, 423, 425, 429, 431, 433, 435, 439, 441, 443, 445, 449, 451, 453, 455, 459, 461, 463, 465, 469, 471, 473, 475, 479, 481, 483, 485, 489, 491, 493, 495, 499, 501, 503, 505, 509, 511, 513, 515, 519, 521, 523, 525, 529, 531, 533, 535, 539, 541, 543, 545, 549, 551, 553, 555, 559, 561, 563, 565, 569, 571, 573, 575, 579, 581, 583, 585, 589, 591, 593, 595, 599, 601, 603, 605, 609, 611, 613, 615, 619, 621, 623, 625, 629, 631, 633, 635, 639, 641, 643, 645, 649, 651, 653, 655, 659, 661, 663, 665, 669, 671, 673, 675, 679, 681, 683, 685, 689, 691, 693, 695, 699, 701, 703, 705, 709, 711, 713, 715, 719, 721, 723, 725, 729, 731, 733, 735, 739, 741, 743, 745, 749, 751, 753, 755, 759, 761, 763, 765, 769, 771, 773, 775, 779, 781, 783, 785, 789, 791, 793, 795, 799, 801, 803, 805, 809, 811, 813, 815, 819, 821, 823, 825, 829, 831, 833, 835, 839, 841, 843, 845, 849, 851, 853, 855, 859, 861, 863, 865, 869, 871, 873, 875, 879, 881, 883, 885, 889, 891, 893, 895, 899, 901, 903, 905, 909, 911, 913, 915, 919, 921, 923, 925, 929, 931, 933, 935, 939, 941, 943, 945, 949, 951, 953, 955, 959, 961, 963, 965, 969, 971, 973, 975, 979, 981, 983, 985, 989, 991, 993, 995, 999$~~

$p \equiv 1, 2, \text{ or } 4 \pmod{7}$

$\Rightarrow$ $p = 2, 11, 23 \text{ work!}$

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

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

$41 \equiv 1 \pmod{4}$
 $41 \equiv 3 \pmod{19}$
 $19 \equiv 3 \pmod{4}$

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

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

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

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

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 ?

$$220 = 2^2 \cdot 55. \text{ Let } q = 55.$$

$$2^{55} \equiv 128 \not\equiv \pm 1 \bmod 221 \quad \left. \begin{array}{l} 2^{55} \equiv 128 \not\equiv \pm 1 \bmod 221 \\ 2^{110} \equiv 30 \not\equiv \pm 1 \bmod 221 \end{array} \right\} \text{ Yes, 2 is a M-R witness!}$$

$$2^{110} \equiv 30 \not\equiv \pm 1 \bmod 221 \quad \left. \begin{array}{l} 2^{55} \equiv 128 \not\equiv \pm 1 \bmod 221 \\ 2^{110} \equiv 30 \not\equiv \pm 1 \bmod 221 \end{array} \right\} 221 \text{ is NOT prime.}$$

- (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 $a=2$.

$$\cdot a^2 = 2^2 = 4, \quad \text{gcd}(4-1, N) = 1$$

$$\cdot a^6 = 4^3 = 64, \quad \text{gcd}(63, N) = 1$$

$$\cdot a^{24} = 64^4 \equiv 1 \bmod 221, \quad \text{gcd}(0, N) = N$$

$$\cdot a^{51} \equiv 1 \bmod 221, \quad \text{gcd}(0, 221) = 1$$

$$\cdot a^{71} \equiv \dots \text{ STOP, use another value!}$$

$$a=3$$

$$\cdot a^2 \equiv 9, \quad \text{gcd}(8, N) = 1$$

$$\cdot a^6 \equiv 9^3 \equiv 66, \quad \text{gcd}(65, N) = 13$$

$$\Rightarrow 13 \mid N$$

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

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?

$$N = 221 = 13 \cdot 17$$

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

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

so NO, cannot use $e = 3$.

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

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

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

We need d s.t. $7d \equiv 1 \pmod{\phi(N) = 192}$.

$$\Rightarrow \boxed{d = 55}$$

(Evidently n otherwise)

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

Cipher: $m^e \pmod{221}$, so $2^7 \equiv 128 \pmod{221}$

Alice decrypts:

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

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

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

we find $d = 173$ so

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

(note $7^5 \equiv 11 \pmod{323}$)

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?

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

$$\text{or } 7.92924 \dots \%$$

(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

$$\pi(400000) - \pi(300000) \text{ primes or}$$

$$\frac{400000}{\ln(400000)} - \frac{300000}{\ln(300000)} = 7221.88 \dots$$

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

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

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 $D \equiv 10 \pmod{221}$. Produce a signature for D .

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

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

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

$$S^e \equiv 192^7 \equiv 10 \equiv D \pmod{221} \quad \checkmark$$

- (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 $D \equiv 10 \pmod{43}$. Produce a signature for D .

$$A \equiv g^a \equiv 3^5 \equiv 28 \pmod{43}$$

$$D \equiv 10 \Rightarrow S_1 \equiv 3^2 \equiv 9 \pmod{43}$$

$$S_2 \equiv (10 - 5 \cdot 9) \cdot 2^{-1} \pmod{42}$$

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 $D \equiv 10 \pmod{43}$. Produce a signature for D .

$$\cancel{A \equiv 28 \pmod{43}}, D \equiv 10, A \equiv g^a \equiv 41^5 \equiv 11 \pmod{43}$$

$$S_1 \equiv (41^2 \pmod{43}) \pmod{7} \equiv 4$$

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

(D, S_1, S_2)
 $(10, 4, 1)$

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

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

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

$$(41^3 \cdot 4^4 \pmod{43}) \equiv 4 \pmod{7} \equiv S_1 \quad \checkmark$$