Math 458, Exam 2
Spring 2019
Instructor: Dugger

Name: Solutions

Instructions: This is a 50 minute exam. You are allowed a 3×5 notecard (front and back) and a calculator. Answers must be accompanied by explanations to earn full credit.

1. (10 points) Is the number $a = 2$ a Miller-Rabin witness for $N = 25$? What about $a = 3$? In each case, explain why or why not.

$N-1 = 24 = 2^3 \cdot 3 \qquad k=3,\ q=3$

$a=2$: $2^3 = 8 \neq 1$

$8,\ 8^2 = 64 = 14,\ 14^2 = 196 = 21$

all not -1 in $\mathbb{Z}/25$

So $a=2$ is M-R witness

$a=3$ $\qquad 3^3 = 27 = 2 \neq 1$

$2,\ 2^2 = 4,\ 4^2 = 16$

all not -1 in $\mathbb{Z}/25$

So $a=3$ is M-R witness

2. (10 points) Suppose you use Pollard's $p-1$ algorithm to factor $N = 341371$. The algorithm tells you the factors are 541 and 631. What value of $n!$ did the algorithm stop at, and which prime factor did it discover first? Explain.

$p-1 = 540 = 54 \cdot 10 = 2 \cdot 3^3 \cdot 2 \cdot 5 = 2^2 \cdot 3^3 \cdot 5$

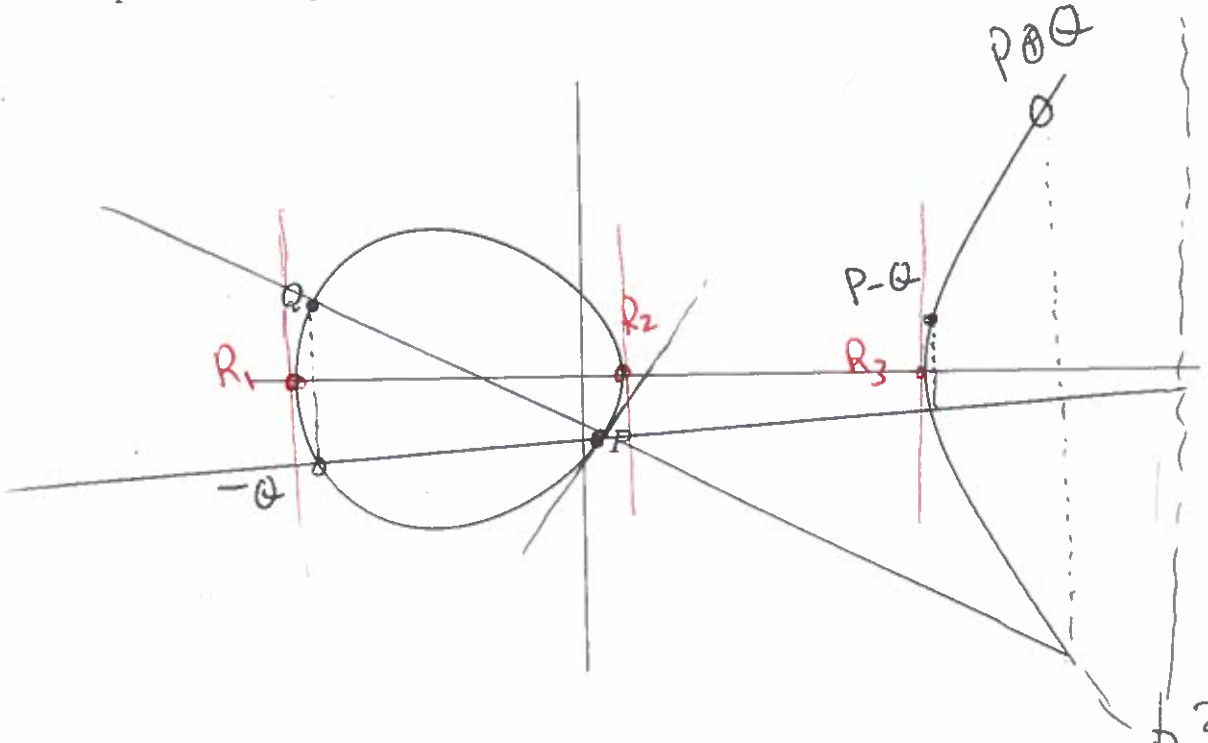
$q-1 = 630 = 63 \cdot 10 = 7 \cdot 3^2 \cdot 2 \cdot 5 = 2 \cdot 3^2 \cdot 5 \cdot 7$

$q-1 \mid 7!$, and this is the smallest factorial that is a multiple of $q-1$

For $p-1$ we need to go to $9!$ to get the 5 and three 3's.

So Pollard algorithm stops at $7!$ and discovers the 631 factor.

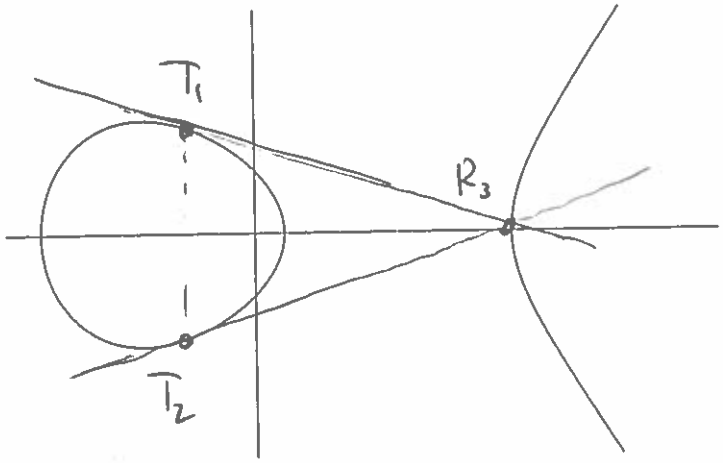
3. (15 points) The following graph shows an elliptic curve $y^2 = x^3 + Ax + B$ over $\mathbb{R}$, with points P and Q marked on it.



(a) On the graph, mark the points $P + Q$, $P - Q$, and $2P$. [You do not have to be super-exact here, but your markings should be roughly correct and also allow me to see how you got your answer.]

(b) Mark all points R on the graph that satisfy $2R = \mathcal{O}$. See graph

(c) Mark two points T on the graph that have not been marked so far and satisfy $4T = \mathcal{O}$. (Hint: If $4T = \mathcal{O}$ then $2(2T) = \mathcal{O}$.) Here is another picture if the above graph has gotten too messy:



$T_1 + T_1 = R_3 = T_2 + T_2$

So $4T_1 = 2R_3 = \mathcal{O}$, $4T_2 = 2R_3 = \mathcal{O}$

4. (15 points) (a) If you randomly pick a number from 1 to 10^6, what is the (approximate) probability that the number is prime, according to the Prime Number Theorem?

$$\text{Prob} = \frac{1}{\ln(10^6)} = \frac{1}{6\ln(10)} \approx 0.072382$$

(b) Suppose you randomly pick such a number and then do this again and again, all in all 10 times. What is the probability that *none* of your numbers was prime?

$$(1-0.072382)^{10} \approx 0.4717259$$

(c) How many times should you do the random picking if you want the probability that none are prime to be smaller than 0.01? Give the smallest number of times that will accomplish this, and explain how you got your answer. (Hint: I suggest keeping 4 or 5 significant digits in your calculations).

$$(1-0.072382)^{k} = (0.927618)^{k}$$

Calculator:

k	power
50	0.023
60	0.011
70	0.0051

61	0.0102
62	0.00948
65	0.007

So $\boxed{k=62}$ is the first time when prob < 0.01

Formula solution: $\left(1-\frac{1}{6\ln 10}\right)^{k} < 0.01$

$$k \cdot \ln\left(1-\frac{1}{6\ln 10}\right) < \ln(0.01) \Rightarrow k > \frac{\ln(0.01)}{\ln\left(1-\frac{1}{6\ln 10}\right)} = \frac{-4.605}{-0.075} = 61.48$$

5. (10 points) Bob uses the RSA algorithm with $N = 11021$ and $e = 983$. He sends a message m to Alice, and the ciphertext that Alice receives is "3". Based on this information, it would be hard for you to decode the original message by hand; but a spy has discovered that one of Bob's secret primes is $p = 103$. Using this, find the number m. [Note: The numbers are chosen so that this can be done in just a few minutes, despite the fact that they look big].

$m^e = 3$ & $p = 103$ $\quad q = \frac{11021}{103} = 107$

Find d s.t $de \equiv 1 \mod (p-1)(q-1) = 102 \cdot 106 = 10812$

(can also use $\text{lcm}(p-1, q-1) = 5406$ here)

$10812 = 983(10) + 982$

$983 = 982(1) + 1$

$\Rightarrow$

$1 = 983 - 982$

$= 983 - (10812 - 983(10))$

$= 11 \cdot 983 - 10812$

So $11 \cdot 983 = 1 \mod 10812$

$\boxed{d = 11}$

Now $m = 3^d = 3^{11} = 177147$

$\equiv 811 \mod 11021$

$\boxed{m = 811}$

6. (15 points) Let E be the elliptic curve $y^2 = x^3 - 7x + 10$ over $\mathbb{F}_{11}$.

(a) $P = (1,2)$ and $Q = (3,7)$ are both points on this curve. Determine $P + Q$.

$\lambda = \frac{7-2}{3-1} = \frac{5}{2} = 5 \cdot 6 = 30 = 8$ in $\mathbb{F}_{11}$ $(2^{-1} = 6)$

$x = \lambda^2 - (1+3) = 64 - 4 = 60 = 5$

$y = \lambda(1-5) - 2 = 8(-4) - 2 = -34 = 10$

$P \oplus Q = (5, 10)$

(b) Suppose I tell you that $7P = (2,9)$. What is $14P$?

$1 = 12 = 23 = 34 = 45 = 56$ (11)

7 · 8

Need to do $(2,9) + (2,9)$

$\lambda = \frac{3(2)^2 + 1 - 7}{2 \cdot 9} = \frac{5}{18} = \frac{5}{7} = 5 \cdot 7^{-1}$ So $7^{-1} = 8$

$= 5 \cdot 8 = 40 = 7$

$x = \lambda^2 - (2+2) = 49 - 4 = 45 = 1$

$y = \lambda(2-1) - 9 = 7 - 9 = -2 = 9$

$(1,9)$

(c) Given as above that $7P = (2,9)$, what is $-7P$?

Recall: If $Q = (a,b)$ then $-Q = (a,-b)$

So $-7P = (2,-9)$