E. Dummit's Math 4527 ~ Number Theory 2, Spring 2021 ~ Homework 6, due Thu Mar 4th.

Justify all responses with clear explanations and in complete sentences unless otherwise stated. Write up your solutions cleanly and neatly, and clearly identify all problem numbers. Either staple the pages of your assignment together and write your name on the first page, or paperclip the pages and write your name on all pages.

Part I: No justifications are required for these problems. Answers will be graded on correctness.

1. Factor the given integers n using the given point P on the elliptic curve E modulo n. Make sure to indicate the divisor found along with the number of iterations required:

   (a) $n = 176140997$, $E : y^2 = x^3 + 2x + 13$, $P = (1, 4)$.

   (b) $n = 88757997707$, $E : y^2 = x^3 + 2x + 13$, $P = (1, 4)$.

   (c) $n = 74148675791$, $E : y^2 = x^3 + 5x - 9$, $P = (2, 3)$.

   (d) $n = 21514038761$, $E : y^2 = x^3 + 5x - 9$, $P = (2, 3)$.

---

2. The Legendre symbol $\left(\dfrac{a}{p}\right)_L$ is defined only when p is a prime number. We can generalize it as follows: if $b = p_1 \cdots p_k$ is a product of (not necessarily distinct) primes p_k, the Jacobi symbol $\left(\dfrac{a}{b}\right)$ is defined as $\left(\dfrac{a}{b}\right) = \left(\dfrac{a}{p_1}\right)_L \cdots \left(\dfrac{a}{p_k}\right)_L$, where $\left(\dfrac{a}{p_k}\right)_L$ denotes the Legendre symbol. Calculate these Jacobi symbols:

   (a) $\left(\dfrac{5}{51}\right)$.

   (b) $\left(\dfrac{3}{51}\right)$.

   (c) $\left(\dfrac{433}{777}\right)$.

   (d) $\left(\dfrac{881}{1101}\right)$.

---

3. One of the most surprising and wonderful theorems in all of number theory is the law of quadratic reciprocity, which says that if p and q are odd primes, then $\left(\dfrac{p}{q}\right)\left(\dfrac{q}{p}\right) = (-1)^{(p-1)(q-1)/4}$, which was discovered and proven by Gauss. If this theorem does not strike you as miraculous, ponder why there would be any relationship at all between whether p is a square modulo q and whether q is a square modulo p, and why the answer could possibly depend on what p and q are mod 4.

   (a) Verify quadratic reciprocity for the primes $p = 17$ and $q = 19$.

   (b) Verify quadratic reciprocity for the primes $p = 23$ and $q = 43$.

   Quadratic reciprocity can be shown to hold for Jacobi symbols too. Using the additional evaluations $\left(\dfrac{-1}{n}\right) = (-1)^{(n-1)/2}$ and $\left(\dfrac{2}{n}\right) = (-1)^{(n^2-1)/8}$ for n odd, one may use quadratic reciprocity to evaluate Jacobi symbols very rapidly.

   - Example: We have $\left(\dfrac{247}{1009}\right) = \left(\dfrac{1009}{247}\right) = \left(\dfrac{21}{247}\right) = -\left(\dfrac{247}{21}\right) = -\left(\dfrac{16}{21}\right) = -1$.

   (c) Use quadratic reciprocity for Jacobi symbols to compute the four Jacobi symbols from problem 2.

---

4. Alice and Bob decide to send some messages using elliptic curve cryptography. They begin by choosing the elliptic curve $E : y^2 = x^3 + Ax + B$ modulo p and compute its number of points N (which is prime):

$$\begin{aligned} p &= 10485767 \\ A &= 6 \\ B &= 6 \\ N &= 10490089. \end{aligned}$$

(a) Alice first wants to convert her plaintext message **test** into a point on the curve. She begins by converting her string into binary one letter at a time (**a** $= 00000$, **b** $= 00001$, ... , **z** $= 11001$) and then writing it in base 2 to obtain

$$m = 10011001001001010011_2 = 627283_{10}.$$

She then wants to pad her message of length $r = 20$ bits with an additional $k = 2$ bits at the beginning to obtain the x-coordinate of a point (x, y) on the curve E modulo p. Find a possibility for the resulting point (x, y).

(b) Alice and Bob next want to use elliptic-curve Diffie-Hellman to construct a shared key. They choose the starting point

$$P = (474566,\ 2794127).$$

Alice chooses $a = 567180$ and Bob chooses $b = 115019$. Identify the two points aP and bP they send to one another and verify that they end up with the same key abP.

(c) Bob next creates an elliptic-curve ElGamal public key with

$$\begin{aligned} Q_a &= (111952, 894486) \\ Q_b = dQ_a &= (4537150, 8707432) \\ d &= 567180. \end{aligned}$$

Alice wants to send Bob the message

$$P = (2490983, 773516).$$

Identify the pair (Q_r, Q_s) Alice will send if she takes her random $k = 7128391$ and verify that it decodes correctly.

(d) Alice sends Bob another message using the same key as in part (c). Her message pair is

$$\begin{aligned} Q_r &= (10140558, 1341676) \\ Q_s &= (10483673, 8827780). \end{aligned}$$

Find Alice's message P and its text decoding, assuming it is encoded using the same procedure as in part (a) with length $r = 20$ bits.

(e) Finally, Alice wants to create an elliptic-curve ElGamal signature, so she first creates her public signature key

$$\begin{aligned} Q_a &= (1193982, 5349155) \\ Q_b = dQ_a &= (775382, 3834766) \end{aligned}$$

with her secret $d = 2213000$. Bob asks for a signature on his message m and Alice responds with

$$\begin{aligned} m &= 8195012 \\ Q_r &= (2265308, 9758754) \\ s &= 9510003. \end{aligned}$$

Verify that Alice has properly signed the message.

Part II: Solve the following problems. Justify all answers with rigorous, clear arguments.

5. Alice wishes to send an encrypted message to Bob using RSA. To do this, Bob chooses two large primes p and q along with an encryption exponent e relatively prime to $\varphi(pq) = (p-1)(q-1)$, and publishes the two values $N = pq$ and e, which are his public key. Alice encrypts her message, which is a residue class m modulo N, by computing the ciphertext $c \equiv m^e \bmod N$, and sends the value c to Bob. To decrypt Alice's message, Bob computes a decryption exponent $d \equiv e^{-1} \pmod{\varphi(N)}$ and evaluates $c^d \pmod{N}$.

   (a) Assuming that $N = pq$ is a product of two primes, show that factoring N is equivalent to computing $\varphi(N)$. [Hint: Find a formula for p and q in terms of $N = pq$ and $\varphi = (p-1)(q-1)$.]

   (b) Suppose that the primes p and q are close to each other, so that $q < p < 2q$, and that Bob has a small decryption exponent: specifically, that $d < \frac{1}{3}N^{1/4}$. Prove that if $k = \frac{de-1}{\varphi(N)}$, then $\frac{k}{d}$ is within $\frac{1}{3d^2}$ of $\frac{e}{N}$. Deduce that k/d is a continued fraction convergent of e/N and describe how this information can be used to calculate $\varphi(N)$.

   (c) Given the RSA public key (e, N) below, and the information that $N = pq$ with $q < p < 2q$ and that the decryption exponent has $d < \frac{1}{3}N^{1/4}$, find the factorization of N.

$$\begin{aligned} N &= 57689254024036183888718503966884177523086419886438161001073372632511969905080297 \\ e &= 25250848999164909164249104247600348919876678272890811307070973522692563710935769 \end{aligned}$$

   - Remark: This attack on RSA is known as Weiner's attack.

---

6. Eve reads about the baby-step giant-step algorithm and decides to adapt it to create an attack on RSA: she knows Bob's public key (N, e) and has a plaintext-ciphertext pair (m, c) and wants to find a decryption exponent d. She chooses an integer M such that $M^2 \geq N$ and then computes two lists: the values $c^x \pmod{N}$ for all $0 \leq x \leq M-1$ and the values $mc^{-My} \pmod{N}$ for all $0 \leq y \leq M-1$.

   (a) Explain why Eve is always guaranteed to find a match between the two lists, and how she can use a match to find an exponent d such that $c \equiv m^d \pmod{N}$. [Hint: Write N in base M.]

   (b) Is the value d from part (a) always guaranteed to be an actual decryption exponent for all ciphertexts? [Hint: What if $m = c = 1$?]

   (c) Explain why this attack will not be a very useful practical attack on RSA. [Hint: How long does it take to compute each list?]

---

7. [Optional but fun] Let p be an odd prime and a be a unit modulo p. Prove Zolotarev's lemma: the sign of the permutation corresponding to multiplication by a on the $p-1$ nonzero residue classes modulo p is equal to the Legendre symbol $\left(\frac{a}{p}\right)$. [Hint: The sign map and the Legendre symbol are both homomorphisms. Compute their values on a primitive root.]

   - Remark: If you look up Zolotarev's lemma on wikipedia, you will find several other proofs, all of which are more difficult than this one.
