Problem 1. (15 points)
(a) Alice decides to use an **RSA digital signature**. She chooses primes $p$ and $q$. What information does she publish for people to use in verifying her signatures?
(b) Alice then decides to sign a digital document $D$. What information does she use to create her digital signature for $D$ and what is the signature?
(c) Explain what quantity Bob computes and how he uses it to verify Alice’s signature on the document $D$.

Solution. (a) Alice publishes $$(N, v),$$ where $N = pq$ and the verification exponent $v$ satisfies $\gcd(v, (p − 1)(q − 1)) = 1$.
(b) Alice finds $s$ satisfying $sv \equiv 1 \ (\mod (p − 1)(q − 1))$. The signature on $D$ is the quantity $S = D^s \mod N$. (For added efficiency, Alice can compute $G = \gcd(p − 1, q − 1)$ and instead use the value of $s$ satisfying $sv \equiv 1 \ (\mod (p − 1)(q − 1)/G)$.)
(c) Bob computes $S^v \mod N$ and checks that it is equal to $D$. 
Problem 2. (10 points) Circle either True or False. You do not have to give a reason. NOTE: Correct answers receive +1, incorrect answers receive −1, unanswered parts receive 0.

(a) If \(2^n \equiv 2 \pmod{n}\), then \(n\) must be prime.  
False. (The smallest counterexample is \(n = 341 = 11 \cdot 31\).)

(b) If \(n\) is prime, then \(3^n\) is congruent to 3 modulo \(n\).  
True, this is a special case of Fermat’s Little Theorem.

(c) There are approximately 1086 primes less than 10000.  
(Hint: 10000 \(\approx e^{9.2}\).)  
True, \(\pi(10000) \approx \frac{10000}{\ln(10000)} \approx \frac{1000}{9.2} \approx 1085.73\).  
The exact value is \(\pi(10000) = 1229\).

(d) There are approximately 4328 primes less than 100000.  
(Hint: 100000 \(\approx e^{11.5}\).)  
False, \(\pi(100000) \approx \frac{100000}{\ln(100000)} \approx \frac{10000}{11.5} \approx 8685.89\), which is not close to 5328. The exact value is \(\pi(100000) = 9592\).

(e) There are approximately \(e^{\sqrt{n} \frac{\ln n}{(\ln \ln n)}}\) primes less than \(x\).  
False, the counting function for primes is \(\pi(x)\), which is approximately equal to \(x/\ln(x)\).

(f) The number 280 is 8-smooth.  
True, since 280 = \(2^3 \cdot 5 \cdot 7\), so every prime dividing 280 is less than or equal to 8.

(g) The number 110 is 10-smooth.  
False, since 110 = \(2 \cdot 5 \cdot 11\) has a prime divisor that is larger than 10, namely 11.

(h) If \(n\) is composite, then there is at least one value of \(a\) satisfying \(a^n \not\equiv a \pmod{n}\).  
False. Carmichael numbers are composite and satisfy \(a^n \equiv a \pmod{n}\) for every value of \(a\).

(i) If \(n\) is composite, then at least \(\frac{3}{4}n\) of the numbers \(2 \leq a < n\) are Miller-Rabin witnesses for the compositeness of \(n\).  
True. It is this important fact that makes the Miller-Rabin test so efficient.

(j) The function \(L(X) = e^{\sqrt{\ln X \ln \ln X}}\) is smaller than \((\ln X)^{10}\) when \(X\) is large.  
False. \(L(X)\) is subexponential, so it is \(O(X^{\epsilon})\) for any \(\epsilon > 0\), but it is not polynomial, so it grows faster than \(O((\ln X)^d)\) for any \(d > 0\).
**Problem 3.** (10 points) (a) Describe *briefly* and *clearly* Pollard’s \( p - 1 \) factorization algorithm.
(b) Describe *briefly* and *clearly* the Rabin–Miller test for compositeness and explain why it can be used to test if a number is probably prime.

**Solution.** (a) Choose some \( a > 1 \) and compute \( \gcd(a^k - 1, N) \) for \( k = 1, 2, 3, \ldots \). To avoid using huge numbers and cut down on the calculations, let \( A_1 = a \), and then for \( k = 1, 2, \ldots \), compute

\[
G = \gcd(A_k - 1, N) \quad \text{and} \quad A_{k+1} = A_k^k \pmod{N}.
\]

If \( 1 < G < N \), the \( G \) is a nontrivial factor of \( N \). This will probably succeed in a reasonable amount of time if \( N \) has a factor \( p \) such that \( p - 1 \) is a product of small primes (to various powers). However, if you ever get \( \gcd(A_k - 1, N) = N \), then you have to go back and choose a different value for \( a \).

(b) First factor \( N - 1 = 2^k q \) with \( q \) odd. Choose a random value \( a \). If

\[
a^q \not\equiv 1 \pmod{N}
\]

and

\[
a^{2^i q} \not\equiv -1 \pmod{N} \quad \text{for all } i = 0, 1, \ldots, k - 1,
\]

then \( a \) is a Miller–Rabin witness for \( N \), and \( N \) is definitely composite. Otherwise choose another random value for \( a \) and try again. If many values of \( a \) fail to show that \( N \) is composite, then \( N \) is probably prime. More precisely, if \( N \) is composite, then at least \( \frac{3}{4} \) of the possible choices for \( a \) are Miller–Rabin witnesses for the compositeness of \( N \).
Problem 4. (10 points) Let $N = 52907$.

(a) Use the following information to find distinct values of $a$ and $b$ that satisfy

$$a^2 \equiv b^2 \pmod{N}.$$ 

- $399^2 \equiv 480 \pmod{52907}$ and $480 = 2^5 \cdot 3 \cdot 5$
- $763^2 \equiv 192 \pmod{52907}$ and $192 = 2^6 \cdot 3$
- $773^2 \equiv 15552 \pmod{52907}$ and $15552 = 2^6 \cdot 3^5$
- $976^2 \equiv 250 \pmod{52907}$ and $250 = 2 \cdot 5^3$

(b) Explain how you would use your answer in (a) to attempt to factor $N$. (NOTE: You do not need to do the computation, just explain what quantity you would compute.)

Solution. (a) There are several possibilities. For example

$$763^2 \cdot 773^2 \equiv (2^6 \cdot 3)(2^6 \cdot 3^5) \equiv (2^6 \cdot 3^3)^2 \equiv 1728^2 \pmod{52907}$$

gives

$$\begin{align*}
a &= 763 \cdot 773 = 589779 \\
b &= 2^6 \cdot 3^3 = 1728.
\end{align*}$$

We note that $a \equiv 7822 \pmod{52907}$, which is different from $b$.

A second possibility is

$$399^2 \cdot 763^2 \cdot 976^2 \equiv (2^5 \cdot 3 \cdot 5)(2^6 \cdot 3)(2 \cdot 5^3) \pmod{52907}$$

$$= (2^6 \cdot 3 \cdot 5^3)^2 = 4800^2,$$

which gives

$$\begin{align*}
a &= 399 \cdot 763 \cdot 976 = 297130512 \\
b &= 2^6 \cdot 3 \cdot 5^2 = 4800.
\end{align*}$$

However, this choice actually won’t lead to a factorization of $N$, because it turns out that $a - b$ is divisible by $N$.

(b) Once we have $a^2 \equiv b^2 \pmod{N}$, we compute $\gcd(N, a - b)$ to try to find a nontrivial factor of $N$. For the exam, you were not required to compute the gcd, but if you did so, you’d find that

$$\gcd(52907, 589799 - 1728) = \gcd(52907, 587997) = 277.$$

Thus $52907 = 277 \cdot 191$. 
Problem 5. (10 points) Alice and Bob decide to use the NTRU public key cryptosystem with the parameters \((N, p, q)\).

(a) Alice’s secret key is \(f(x)\), and she also knows a polynomial \(F_p(x)\) that satisfies \(f(x) \star F_p(x) \equiv 1 \pmod{p}\). If Bob sends Alice the ciphertext \(e(x)\), explain what Alice computes to recover Bob’s plaintext.

(b) Alice and Bob use the parameters \((N, p, q) = (3, 2, 5)\).

(Yes, I know, these parameters are much too small to be secure!) Alice’s public key is
\[
h(x) = x^2 + 2x + 2.
\]
Bob wants to send Alice the plaintext
\[
m(x) = x^2 + 1,
\]
using the random (ephemeral) key \(r(x) = x - 1\).

What is the ciphertext that Bob sends to Alice?

Solution. (a) Alice first computes \(a(x) \equiv f(x) \star e(x) \pmod{q}\), always keeping in mind that \(x^N = 1\) to simplify the answer. She next centerlifts, which means that she takes the coefficients of \(a(x)\) to be between \(-q/2\) and \(q/2\). She then computes \(F_p(x) \star a(x)\) and reduces the coefficients modulo \(p\). This gives Bob’s plaintext \(m(x)\).

(b) The NTRU ciphertext is given by the formula
\[
e(x) \equiv pr(x) \star h(x) + m(x) \pmod{q}.
\]
So Bob first computes
\[
r(x) \star h(x) = (x^2 + 2x + 2) \star (x - 1)
\]
\[
= x^3 + 2x^2 + 2x - x^2 - 2x - 2
\]
\[
= x^3 + x^2 - 2
\]
\[
= x^2 - 1,
\]
where for the last equality Bob uses the fact that \(x^N - 1 = 0\), which for the given parameters means that \(x^3 = 1\). Next Bob multiplies by \(p\) and adds \(m(x)\) to get the ciphertext
\[
e(x) = pr(x) \star h(x) + m(x) = 2(x^2 - 1) + (x^2 + 1) = 3x^2 - 1.
\]
Of course, the ciphertext is really modulo \(q\), where for this problem \(q = 5\), so if Bob wants to use positive coefficients, he can instead use \(e(x) = 3x^2 + 4\).