Problem 1 (10 points)

Solution 1

We calculate the expected (average) value of the number of times we must toss a coin before it comes up heads. Let X be the random variable corresponding to the number of tosses needed before coming up heads.

$$E[X] = \sum_{i=1}^{\infty} i \cdot P[X = i]$$

We now calculate $P[X = i]$: For a coin to come up heads (for the first time) in exactly i tosses, we must have $i - 1$ tails followed by one head. It follows that $P[X = i] = (1 - p)^{(i-1)}p$, for $i \geq 1$. So,

$$E[X] = \sum_{i=1}^{\infty} i \cdot (1 - p)^{(i-1)}p = p \cdot \frac{d}{dp}(\sum_{i=0}^{\infty} -(1 - p)^i)$$

The above power series $\sum_{i=0}^{\infty} -(1 - p)^i$ converges for $0 < p < 1$ and it is equal to $-\frac{1}{1-(1-p)} = -\frac{1}{p}$. After taking the derivative, we obtain

$$E[X] = p \cdot \frac{1}{p^2} = \frac{1}{p}$$

Solution 2

Let X be the random variable as in solution 1. Then $E[X]$ the average number of tosses, with each possibility weighted by its probability. With probability p we get heads in one toss of the coin and with probability $1 - p$, we get tails and need to start again and do another $E[X]$ on average (hence we do a total of $E[X] + 1$ tosses with probability $1 - p$). Therefore $E = p \cdot 1 + (1 - p) \cdot (1 + E) = 1 + (1 - p)E$. Solving for E, we get $E = 1/p$.

Problem 2 (10 points)

(a) **(3 points).** Assume that N consists of n bits. We can then perform a binary search on the interval $[2^n - 1, 1]$ to find if it contains a number q such that $q^2 = N$ (binary search is applicable in this case because for positive integers a and b, $a < b$ implies $a^2 < b^2$). Every iteration takes time $O(n^2)$ to square the current element and $O(n)$ to compare the result with N. As there are $O(\log 2^n) = O(n)$ iterations, the total running time is $O(n^3)$.

(b) **(3 points).** $N = q^k \Rightarrow \log N = k \log q \Rightarrow k = \frac{\log N}{\log q} \leq \log N$ for all $q \geq 2$ (this is because our logs are to base 2, and so $q \geq 2$ implies $\log q \geq 1$). If $q = 1$, then we must have $N = 1$.

(c) **(4 points).**We first give an algorithm to determine if a n-bit number N is of the form q^k for some given k and $q > 1$. For this , we use the same algorithm as part (a); only instead of squaring, we will raise numbers to the k-th power and check if we obtain N. This will take $O(n)$ iterations: moreover, each powering operation takes time at most $\sum_{i=1}^{k}(in \cdot n) = O(k^2n^2)$. Hence, one run of this algorithm takes time $O(k^2n^3)$. To check if N is a power, we need to repeat this for all $k \leq \log N \leq n$. This yields a running time of $O(n^6)$.

This running time can be improved further, by stopping each powering iteration once the number of bits of an intermediate product is larger than n. If the product is done via repeated squaring, this means that the last multiplication (which dominates the total cost) is between two numbers with at most n-bits. Therefore, the total powering cost is $O(n^2)$, yielding an algorithm with a running time of $O(n^4)$. Repeated squaring is not actually necessary and the iterative cost can be shown to be the same if this technique is used. However we will award full credit for the first solution as well.

Problem 3 (10 points)

(a) **(4 points).** Since a is a non-zero quadratic residue $\mod N$, there exists $x \in \{1, \ldots, N-1\}$ such that $x^2 \equiv a \mod N$ (because $a \neq 0$ implies we cannot have $x = 0$). Notice that we also have $(N-x)^2 \equiv x^2 \mod N \equiv a \mod N$, and also that $(N-x) \in \{1, \ldots, N-1\}$. We will now show that when N is odd, $x \neq N - x$. For if not, then we have $x = N - x$, so that $N = 2x$ which contradicts the fact that N is odd. Thus, we have at least two distinct values for $x \in \{1, 2, \ldots, N-1\}$ which satisfy $x^2 \equiv a \mod N$.

We will now show that these are the only possible solutions. Consider any other value $y \in \{1, 2, \ldots, N-1\}$ such that $y^2 \equiv a \mod N$. We then have $x^2 \equiv y^2 \mod N$, so that N divides $x^2 - y^2 = (x-y)(x+y)$. Since N is a prime, this implies that N divides at least one of $x - y$ and $x + y$. We now consider both these cases.

- N **divides** $x - y$**.** If N divides $x - y$, then we see that $x \equiv y \mod N$ which implies that $x = y$, since both x and y are in the set $\{1, 2, \ldots, N-1\}$.
- N **divides** $x + y$**.** Since both x and y are in $\{1, 2, \ldots, N-1\}$, we have $0 < x + y < 2N$, so that N can divide $x + y$ if and only if $x + y = N$. But then we have $y = N - x$.

We therefore see that x and $N - x$ are the only possible solutions. This completes the proof.

(b) **(3 points).** Clearly 0 is a quadratic residue since $0^2 = 0 \mod N$. Now let $S = \{1, 2, \ldots, (N-1)/2\}$. Notice that since N is odd, we have $|S| = (N-1)/2$. From the first part, we know that for an odd prime N, and for $x, z \in \{1, 2, \ldots, N-1\}$, we have $x^2 \equiv z^2 \mod N$ if and only if either $x = z$ or $x + z = N$. Since $x + z < N$ for $x, z \in S$, this implies that for two distinct elements x and z in S, we have $x^2 \not\equiv z^2 \mod N$. We therefore conclude that the set $T = \{x^2 | x \in S\}$ is of size $|S| = (N-1)/2$. Since every element of T is a non-zero quadratic residue, this shows that there are at least $(N-1)/2$ quadratic residues.

We will now show that all the non-zero quadratic residues are contained in T. Consider any non-zero quadratic residue $a \equiv y^2 \mod N$, where $y \in \{1, 2, \ldots, N-1\}$. If $y \in S$, then $a \in T$, by definition. Otherwise, we have $(N+1)/2 \leq y \leq N-1$, so that $N - y \in S$, and hence $a \equiv (N-y)^2 \mod N$ is again in T. Thus, the set T contains all the non-zero quadratic residues. We therefore get that the number of all quadratic residues is $|\{0\} \cup T| = 1 + (N-1)/2 = (N+1)/2$, as required.

(c) **(3 points).** Clearly we cannot take $N = 2$ or an odd prime. We take $N = 8$, and notice that for any odd number b, $b^2 \equiv 1 \mod 8$. Thus, the equation $x^2 = 1 \mod 8$ has *four* solutions $\{1, 3, 5, 7\}$ in the set $\{0, 1, 2, \ldots, 7\}$.

Problem 4 (10 points)

(a) **(4 points).** We first note the prime factorization of 35: $35 = 5 \times 7$. Thus, an integer M is divisible by 35 if and only if M is divisible by *both* 5 and 7. We also know from Fermat's little theorem that for a coprime to 5, we have $a^4 \equiv 1 \mod 5$. Using this, we now calculate:

$$2013^{2014} \mod 5 \equiv 3^{2012+2} \mod 5 \equiv \left(3^{503}\right)^4 \cdot 3^2 \mod 5 \equiv 1 \cdot 3^2 \mod 5 \equiv 4 \mod 5. \quad (1)$$

Similarly,

$$2012^{2013} \mod 5 \equiv 2^{2012+1} \mod 5 \equiv \left(2^{503}\right)^4 \cdot 2^1 \mod 5 \equiv 1 \cdot 2 \mod 5 \equiv 2 \mod 5. \quad (2)$$

Denoting $2013^{2014} - 2012^{2013}$ by M, we then combine eqs. (1), (2) to get that $M \equiv 4 - 2 \equiv 2 \mod 5$. Thus, 5 does not divide M, and hence 35 does not either.

(b) **(6 points).** From Fermat's little theorem, we know that if a is coprime to 5, we have $a^4 \equiv 1 \mod 5$ (since 5 is a prime). To use this fact, we would like to represent $E := 170^{70}$ as $4s+t$, for some positive integer s and some $t \in \{0,1,2,3\}$. Given such a representation, we would get from Fermat's little that

$$2^E \mod 5 \equiv (2^s)^4 \cdot 2^t \mod 5 \equiv 1 \cdot 2^t \mod 5. \tag{3}$$

In order to determine $t \equiv E \mod 4$, we note that $E = 170^{70} = (2 \cdot 85)^{2 \cdot 35} = \left((2 \cdot 85)^2\right)^{35}$, so that

$$E \mod 4 \equiv \left((2 \cdot 85)^2\right)^{35} \mod 4 \equiv \left(4 \cdot 85^2\right)^{35} \mod 4 \equiv 0 \mod 4.$$

Thus, we get that $t = 0$. Substituting this in eq. (3), we get that $2^E \equiv 1 \mod 5$, so that the remainder when it is divided by 5 is 1.

Problem 5 (10 points)

Since d is the multiplicative inverse of $e \mod (p-1)(q-1)$, we know that,

$$ed - 1 = 0 \mod (p-1)(q-1),$$

which means for some positive integer k,

$$ed - 1 = k(p-1)(q-1) \tag{4}$$
$$\implies k = \frac{ed-1}{(p-1)(q-1)}$$

Since $d < (p-1)(q-1)$, and $e = 3$, we get

$$k < \frac{3(p-1)(q-1)-1}{(p-1)(q-1)} < 3 - \frac{1}{(p-1)(q-1)},$$

which implies that $k \in \{1,2\}$. Now, for each $k \in \{1,2\}$ we can use eq. (4), which now has only 2 unknowns (p and q) in conjunction with equation $N = pq$, to solve for p and q. To do this, consider one of the two fixed values of k, and substitute $N = pq, e = 3$ into eq. (4) to obtain the following quadratic equation for p:

$$kp^2 - c_k p + kN = 0, \text{ where } c_k := k(N+1) - (3d-1),$$

which has the solutions

$$p_k = \frac{c_k \pm \sqrt{c_k^2 - 4k^2N}}{2k}.$$

Using the result of Problem 2, we can efficiently determine if the solutions p_k are integral for a given value of k. Our arguments above show that at least one of the p_k's will yield the desired non-trivial factors of N.

Problem 6 (10 points)

(a) **(5 points).** When Eve intercepts the encrypted message $M^e \mod N$ sent by Alice to Bob, she can just ask Bob to sign it for her with his private key, to obtain $(M^e)^d \mod N = M$, by the correctness of the RSA cryptosystem.

(b) **(5 points).**

In this case, Eve can pick k coprime to N at random and ask Bob to sign $M^e \cdot k^e \mod N$. This will yield $(Mk)^{ed} \mod N = Mk \mod N$. Then Eve can use Extended Euclid to obtain $k^{-1} \mod N$ and multiply by such inverse to find M. Notice that in this way Bob's signatures are distributed uniformly over all numbers invertible $\mod N$, as Mk is equally likely to be any of such numbers.