CS 4390/5390 Fall 2013
Shirley Moore, Instructor
Homework 4 Answers

1. Unknown. This statement is Goldbach's Conjecture. See http://mathworld.wolfram.com/GoldbachConjecture.html .

2. True. Consider the sequence $(N+1)!+k,\ k=2,\ldots,N+1$. Each integer in the sequence is composite (since it is divisible by *k*) and there are *N* of them.

3. True. Every integer greater than or equal to 5 can be expressed as one of 6k-1, 6k, 6k+1, 6k+2, 6k+3, 6k+4 for some $k \geq 1$. All but 6k-1 and 6k+1 are composite. Thus any prime greater than 3 can be expressed as one of 6k-1 or 6k+1 for some $k \geq 1$.

4. Unknown. This statement is the twin prime conjecture. See http://mathworld.wolfram.com/TwinPrimeConjecture.html .

5. Unknown. See http://mathworld.wolfram.com/FibonacciPrime.html .

6.

7. (b) There are 245 2-pseudoprimes below 1,000,000 and 246 3-pseudoprimes below 1,000,000.
(c) There are 46 2-spsp's below 1,000,000 and 73 3-spsp's below 1,000,000. Since 1,000,001 is odd and composite and $\phi(1{,}000{,}001) = 990{,}000$, Theorem 5..7 says that there cannot be more than 990,000/4 = 247,500 strong liars below 1,000,000 for any base b. The results for b = 2 and b = 3 are far below this upper bound.

8. We need to show that $m^{ed} \equiv m \pmod{n}$ for all m such that $0 \leq m < n < m^e$, where n, e, and d are as given in the RSA algorithm. We know
(1) n = pq, where p and q are distinct primes
(2) $\gcd(e, \phi(n)) = 1$
(3) $de \equiv 1 \pmod{\phi(n)}$
Case 1. m is relatively prime to n. From (3), we have $de = k \cdot \phi(n) + 1$ for some integer k. Then $m^{de} = m^{\phi(n)\cdot k+1} = (m^{\phi(n)})^k m \equiv 1^k m \pmod{n} = m \pmod{n}$ since $m^{\phi(n)} \pmod{n} \equiv 1$ by Euler's Theorem.
Case 2. If m and n are not relatively prime, then either p divides m or q divides m (but not both since m < n). Without loss of generality, assume p divides m. The p also divides m^{de} so (4) $m^{de} \equiv m \pmod{p}$. Since q does not divide m, by Fermat's Little Theorem, $m^{q-1} \equiv 1 \pmod{q}$. We know $\phi(n) = \phi(p)\phi(q)$ divides $de - 1$ so $\phi(q) = q - 1$ divides $de - 1$, that is $de - 1 = k(q-1)$ for some integer k. Then (5) $m^{de} = m^{(de-1)}m = m^{(q-1)k}m \equiv m \pmod{q}$. Combining (4) and (5), we have $m^{de} \equiv m \pmod{pq} = m \pmod{n}$. (To combine (4) and (5), we used the congruence

property that if m and n are relatively prime and if $a \equiv b \pmod{n}$ and $a \equiv b \pmod{m}$, then $a \equiv b \pmod{mn}$ which is easily proved).

9. This problem illustrates an attack on RSA encryption known at the iterated encryption attack. The attack is based on the cyclic structure of $\mathbf{Z}^*_{\phi(n)}$, where $\mathbf{Z}^*_{\phi(n)}$ is the reduced residue set modulo $\phi(n)$. To carry out the attack, the attacker intercepts $c = m^e \pmod{n}$ and repeatedly performs the encryption operation $E(x) = x^e \pmod{n}$. After k-1 iterations by the attacker, we have $E^k(m) = m^{e^k} \pmod{n}$. The attacker continues until either giving up or finding k such that $E^k(m) = m^e \pmod{n}$. Such a k must exist since $\gcd(e, \phi(n)) = 1$ implies that $e, e^2, \ldots, e^k, \ldots$ are all nonzero in $\mathbf{Z}^*_{\phi(n)}$ and therefore must be cyclic. Let $k = ord_{\phi(n)} e + 1$. Then $e^{k-1} = e^{ord_{\phi(n)} e} \equiv 1 \pmod{\phi(n)}$ and $E^k(m) = m^{e^k} \pmod{n} = (m^{e^{k-1}})^e \pmod{n} \equiv m^e \pmod{n}$. So the decryption key d is $d = e^{k-2} \pmod{\phi(n)}$.

Example: Choose p = 13, p = 17, $n = p \cdot q = 13 \cdot 17 = 221$. Then $\phi(221) = \phi(13)\phi(17) = 12 \cdot 16 = 192$. Choose e = 7. Then using the extended Euclidean algorithm we find d = 55 such that $de \equiv 1 \pmod{192}$. Let m = 42 be the message we wish to encrypt. Then $c = 42^7 \pmod{221} \equiv 185$ is the encrypted message. Since $ord_{192} 7 = 8$, repeating this process 7 more times yields $42^{7^8} \pmod{221} = 42$ and the decryption key is $d = 7^7 \pmod{192} = 55$.