

1. Each item is 2.5 points.

- (a) The gcd has the min power in each exponent while the lcm has the max: gcd $\boxed{2^3 3^2 5^4}$, lcm $\boxed{2^4 3^3 5^4 7^1 11^1}$.
 - (b) $\boxed{\text{No}}$: 30 and 42 not relatively prime.
 - (c) By Euclid, $71 = 14 \cdot 5 + 1$, $5 = 5 \cdot 1$ so $1 \equiv -14 \cdot 5 \pmod{71}$ so inverse is $\boxed{-14 = 57}$.
 - (d) Since $\varphi(25) = 20$, we have $6^{20} \equiv \boxed{1} \pmod{25}$ by Euler's theorem.
 - (e) If $x = 0.\overline{125}$ then $990x = 1000x - 10x = 125.\overline{25} - 1.\overline{25} = 124$, so $x = \boxed{124/990 = 62/495}$.
 - (f) $\varphi(121) = \varphi(11^2) = (11^2 - 11) = \boxed{110}$.
-

2. Induct on n . Base case $n = 1$: $1 + \frac{1}{2} = 2 - \frac{1}{2}$ is true. Inductive step: If $1 + \frac{1}{2} + \frac{1}{4} + \cdots + \frac{1}{2^n} = 2 - \frac{1}{2^n}$, then $1 + \frac{1}{2} + \frac{1}{4} + \cdots + \frac{1}{2^n} + \frac{1}{2^{n+1}} = 2 - \frac{1}{2^n} + \frac{1}{2^{n+1}} = 2 - \frac{1}{2^{n+1}}$ as required.

3. Induct on n . Base cases $n = 1$ ($d_1 = 2 = 2^1$) and $n = 2$ ($d_2 = 4 = 2^2$) hold. Inductive step: if $d_n = 2^n$ and $d_{n-1} = 2^{n-1}$ then $d_{n+1} = 2^n + 2(2^{n-1}) = 2^n + 2^n = 2^{n+1}$ as required. (Note that two base cases are required because the inductive step uses the two previous cases.)

4. Each part is 4 points.

- (a) Euclid: $921 = 5 \cdot 177 + 36$, $177 = 4 \cdot 36 + 33$, $36 = 1 \cdot 33 + 3$, $33 = 11 \cdot 3$. So gcd is $\boxed{3}$; then lcm is $\boxed{921 \cdot 177/3}$.
 - (b) Second congruence has solution $n = 3 + 20a$. Plug into $n \equiv 4 \pmod{19}$ to get $3 + 20a \equiv 4 \pmod{19}$ so $a \equiv 1 \pmod{19}$ yielding $n \equiv \boxed{23 \pmod{380}}$.
 - (c) Order divides $\varphi(55) = \varphi(5)\varphi(11) = 4 \cdot 10 = 40$. Successive squaring gives $2^2 \equiv 4$, $2^4 \equiv 16$, $2^8 \equiv 16^2 \equiv 256 \equiv -19$, $2^{16} \equiv (-19)^2 \equiv 289 \equiv -24$. Then we see $2^{20} \equiv 2^{16} 2^4 \equiv (-24)(16) \equiv -384 \equiv 1$ so order divides 20. But $2^{20/2} \equiv 2^8 2^2 \equiv (-19)(4) \equiv -76$ and $2^{20/5} \equiv 16$ so order is exactly $\boxed{20}$.
-

5. Parts (a) and (b) are each 5 points while (c) is 6 points.

- (a) Note $p|a \cdot a$, so since p is prime then $p|a$ or $p|a$ by the prime divisibility property. Since the two conclusion statements are the same, we have $p|a$.
 - (b) If p is prime and $p|k^2$ and $p|(k+1)^2$ then by (a) we have $p|k$ and $p|(k+1)$ so that $p|(k+1) - k = 1$, impossible. So no primes divide both k^2 and $(k+1)^2$ hence they are relatively prime.
 - (c) Let p be prime. If p divides a, b then p^2 hence p divides a^2, b^2 . Conversely, if p divides a^2, b^2 then p divides a, b by part (a). We conclude that a, b have a prime factor in common if and only if a^2, b^2 do, so a, b are relatively prime if and only if a^2, b^2 are.
-

6. If $a|c$ then write $c = ka$. Since then $b|ka$ and b is relatively prime to a , b divides k by the relatively prime divisibility property. Setting $k = lb$ we have $c = lab$ and so $ab|c$.

7. By Euler, $a^4 \equiv 1 \pmod{5}$ for every unit, and $0^4 \equiv 0 \pmod{5}$, so a^4 is always 0 or 1 mod 5. Then the sum of three fourth powers is 0, 1, 2, or 3 mod 5, hence cannot be 2028 since 2028 is 4 mod 5.

8. If $p \leq 100$ is prime then $p|99!$ so p does not divide $99! - 1$. By Wilson's theorem, $99! \equiv 100!/100 \equiv 100/100 \equiv 1 \pmod{101}$, so 101 does divide $99! - 1$. So 101 is the smallest prime divisor of $99! - 1$.

9. Note $\varphi(18) = 6$. Then $5^6 \equiv 1 \pmod{18}$ by Euler, but $5^2 \equiv 7$ and $5^3 \equiv -1 \pmod{18}$, so the order does not divide 2 or 3, hence must be 6.

10. Each item is worth 3 points.

- (a) Using the Fermat factorization method allows us to factor an integer $N = pq$ where p, q are close together by testing whether $a^2 - N$ is a square for $a > \sqrt{N}$.
 - (b) Using primality/compositeness tests like the Fermat test, the Lucas primality criterion, Miller-Rabin, or AKS allow for rapid and accurate testing of primality even for very large integers.
 - (c) RSA is believed difficult to break on a general message. Finding a general decryption exponent is essentially equivalent in most cases to calculating $\varphi(N)$ which as shown on the homework is equivalent to factoring N .
-

1. Each item is 2.5 points.

- (a) Units (relatively prime to 14) are $\{\overline{1}, \overline{3}, \overline{5}, \overline{9}, \overline{11}, \overline{13}\}$, zero divisors (not relatively prime) are $\{\overline{2}, \overline{4}, \overline{6}, \overline{7}, \overline{8}, \overline{10}, \overline{12}\}$.
 (b) Since 47 is prime, we have $2^{47} \equiv \boxed{2} \pmod{47}$ by Fermat's little theorem.
 (c) Since 11 is prime, we have $10! \equiv \boxed{10} \pmod{11}$ by Wilson's theorem.
 (d) Note $2^{12} \equiv 1 \pmod{13}$ by Euler's theorem, but we can calculate $2^6 \equiv 64 \equiv -1 \pmod{13}$ and $2^4 \equiv 3 \pmod{13}$ so 2 has order $\boxed{12}$.
 (e) $\boxed{3}$ or $\boxed{5}$, since they are the only elements with order 6 modulo 7.
 (f) 10 has order 2 mod 11, so $7/11$ has period $\boxed{2}$. (In fact $7/11 = 0.\overline{63}$.)
-

2. Applying the Euclidean algorithm to $a = 12445$ and $b = 5567$ yields $12445 = 2 \cdot 5567 + 1311$, $5567 = 4 \cdot 1311 + 323$, $1311 = 4 \cdot 323 + 19$, $323 = 17 \cdot 19$ the gcd is $\boxed{19}$. Solving for the remainders gives $1311 = 1 \cdot 12445 - 2 \cdot 5567$, $323 = 5567 - 4 \cdot 1311 = -4 \cdot 12445 + 9 \cdot 5567$, and $19 = 1311 - 4 \cdot 323 = \boxed{17 \cdot 12445 - 38 \cdot 5567}$.

3. Note that $a^3 \equiv a \pmod{3}$ by Fermat, and also $a^2 \equiv a \pmod{2}$ so $a^3 \equiv a^2 \equiv a \pmod{2}$ also by Fermat. So $a^3 - a$ is divisible by both 2 and 3 hence by 6. (Alternatively, just check $a^3 \equiv a$ for all 6 residue classes modulo 6.)

4. Each item is worth 3 points.

- (a) By Euclid, $25 = 2 \cdot 11 + 3$, $11 = 3 \cdot 3 + 2$, $3 = 1 \cdot 2 + 1$, $2 = 2 \cdot 1$. Solving for remainders gives $3 = 1 \cdot 25 - 2 \cdot 11$, $2 = -3 \cdot 25 + 7 \cdot 11$, $1 = 4 \cdot 25 - 9 \cdot 11$ so $-9 \cdot 11 \equiv 1 \pmod{25}$ so inverse is $\boxed{-9 = \overline{16}}$.
 (b) Cancel 2 to get $3n \equiv 5 \pmod{50}$, then multiply by $3^{-1} \equiv 17 \pmod{50}$ to get $n \equiv \boxed{35 \pmod{50}}$.
 (c) Second congruence has solution $n = 7 + 14a$. Plug into first congruence to obtain $7 + 14a \equiv 2 \pmod{9}$ hence $5a \equiv -5 \pmod{9}$ yielding $a \equiv -1 \pmod{9}$ and then $n \equiv \boxed{119 \pmod{126}}$.
 (d) $\varphi(5^5 7^{10}) = \boxed{(5^5 - 5^4)(7^{10} - 7^9) = 24 \cdot 5^4 \cdot 7^9}$.
-

5. Each item is worth 8 points.

- (a) Induct on n . Base case $n = 1$ holds since $F_1 + F_3 = 3 = F_4$. Inductive step: if $F_1 + \cdots + F_{2n+1} = F_{2n+2}$ then $F_1 + \cdots + F_{2n+1} + F_{2n+3} = [F_1 + \cdots + F_{2n+1}] + F_{2n+3} = F_{2n+2} + F_{2n+3} = F_{2n+4}$.
 (b) Induct on n . Base cases $n = 1$ and $n = 2$ have $c_1 = 2 = 2^{F_1}$ and $c_2 = 2 = 2^{F_2}$ as required. Inductive step: if $c_n = 2^{F_n}$ and $c_{n-1} = 2^{F_{n-1}}$ then $c_{n+1} = c_n c_{n-1} = 2^{F_n} 2^{F_{n-1}} = 2^{F_n + F_{n-1}} = 2^{F_{n+1}}$. (Note that two base cases are required because the inductive step uses the two previous cases.)
-

6. If $a = b$ then $\gcd(a, a) = a = \text{lcm}(a, a)$. Conversely, if $\gcd(a, b) = \text{lcm}(a, b)$ then every prime must appear to the same power in the prime factorizations of a and b (since otherwise the higher power would be the power in the lcm and the lower power would be the power in the gcd), hence $a = b$.

7. Note $3^1 \equiv 3 \pmod{61}$, $3^2 \equiv 9 \pmod{61}$, $3^4 \equiv 81 \equiv 20 \pmod{61}$, $3^8 \equiv 20^2 \equiv 400 \equiv 34 \pmod{61}$. So $3^{10} \equiv 3^8 \cdot 3^2 \equiv 34 \cdot 9 \equiv 1 \pmod{61}$ so the order divides 10. But $3^5 \equiv 3^4 \cdot 3 \equiv 60 \pmod{61}$ and $3^2 \equiv 9 \pmod{61}$, so the order does not divide 2 or 5, so it is 10.

8. Suppose $xy \equiv 0 \pmod{m}$. Then $(ux)y \equiv u(xy) \equiv u0 \equiv 0 \pmod{m}$, and also $ux \not\equiv 0$ since if $ux \equiv 0$ then $x \equiv u^{-1}(ux) \equiv 0$, contradiction. So ux is a zero divisor. (Alternatively, if $\gcd(x, m) = d > 1$, then d divides ux and m so $\gcd(ux, m) > 1$.)

9. Let $x = a^{(p-1)/2}$; then $x^2 \equiv a^{p-1} \equiv 1 \pmod{p}$ by Euler. Thus $p \mid (x^2 - 1)$ so $p \mid (x - 1)$ or $p \mid (x + 1)$ so $x \equiv 1$ or $-1 \pmod{p}$ (as in 5(a) on HW5). But since a has order $p - 1$, we see $x = a^{(p-1)/2}$ cannot be $1 \pmod{p}$, and so $x \equiv -1 \pmod{p}$.

10. Each item is worth 3 points.

- (a) The Euclidean algorithm is very efficient for computing gcds even for large numbers. (Finding gcds via prime factorization, on the other hand, is very slow.)
 (b) Trial division is slow for 40-digit integers, but Pollard ρ / sieving works well on numbers of that size (Pollard ρ takes $\sim N^{1/4}$ time to factor N , which for $N \approx 10^{40}$ gives a computation size of $\approx 10^{10}$ steps, very doable).
 (c) Finding the four decodings of a single Rabin ciphertext c allows rapid factorization of the modulus: if the decodings are $\pm m$ and $\pm w$ then $\gcd(m + w, N)$ will be a prime factor of N . If Eve is able to obtain the four decodings of some c , she can factor N : for this reason Rabin encryption is not suitable for modern use.
-