1. Use the extended Euclidean algorithm to calculate the gcd and write it as a linear combination:
   (a) gcd $4 = 4 \cdot 12 - 1 \cdot 44$
   (b) gcd $6 = -168 \cdot 20223 + 1681 \cdot 2022$
   (c) gcd $19 = 17 \cdot 12445 - 38 \cdot 5567$,
   (d) gcd $1 = -55 \cdot 233 + 89 \cdot 144$.

---

2. In general $\overline{a}$ is a unit modulo m if and only if a is relatively prime to m. In this case use Euclid to write the gcd 1 as a linear combination $1 = xa + ym$: then $xa \equiv 1 \pmod{m}$ so $x = a^{-1}$.
   (a) No, 10 and 25 not relatively prime.
   (b) Yes, by Euclid, inverse is $\overline{16}$.
   (c) Yes, by Euclid, inverse is $\overline{23}$.
   (d) No, 30 and 42 not relatively prime.
   (e) Yes, by Euclid, inverse is $\overline{19}$.
   (f) No, 32 and 42 not relatively prime.

---

3. Note that the order of any element modulo m divides $\varphi(m)$. We can then evaluate $a^{\varphi(m)/p}$ for primes p dividing $\varphi(m)$ to find the order. Also, if a has order n, then a^k has order $n/\gcd(n, k)$.
   (a) Note $2^{12} \equiv 1$, but $2^6 \equiv -1$, $2^4 \equiv 3$ so 2 has order 12. Also $3^3 \equiv 1$ and $3^1 \equiv 3$ so 3 has order 3.
   (b) Note $2^4 \equiv -1$ so $2^8 \equiv 1$ so 2 has order 8. Then $4 = 2^2$ has order $8/\gcd(2, 8) = 4$ while $8 = 2^3$ has order $8/\gcd(3, 8) = 8$.
   (c) Note $2^4 \equiv 1$ but $2^2 \equiv 4$ so 2 has order 4. Then $4 = 2^2$ has order 2, while $8 = 2^3$ has order 4.
   (d) Note $3^4 \equiv 1$ but $3^2 \equiv 9$ so 3 has order 4. Also $5^2 \equiv 9$ so $5^4 \equiv 1$ so 5 also has order 4. But $15 \equiv -1$ has order 2.
   (e) Use successive squaring: note $5^2 \equiv 3$ so $5^4 \equiv 9$ and thus $5^5 \equiv 1$, so 5 has order 5.
   (f) Note $2^2 \equiv 4$, $2^4 \equiv 16$, $2^8 \equiv -19$, $2^{16} \equiv -24$, so $2^5 \equiv 32$, $2^{10} \equiv -1$, and $2^{20} \equiv 1$. Thus, 2 has order 20. Then $4 = 2^2$ has order 10, $8 = 2^3$ has order 20, $16 = 2^4$ has order 5, and $32 = 2^5$ has order 4.

---

4. Here are answers with brief comments about the approach:
   (a) By Euclid, gcd 8, lcm $256 \cdot 520/8$.
   (b) By Euclid, gcd 3, lcm $921 \cdot 177/3$.
   (c) The gcd has the min power in each exponent while the lcm has the max: gcd $2^3 3^2 5^4$, lcm $2^4 3^3 5^4 7 \cdot 11$.
   (d) We have $\overline{4} + \overline{6} = \overline{10} = \overline{2}$, $\overline{4} - \overline{6} = \overline{-2} = \overline{6}$, $\overline{4} \cdot \overline{6} = \overline{24} = \overline{0}$.
   (e) By Euclid, we get $\overline{4}^{-1} \equiv \overline{18}$, $\overline{5}^{-1} \equiv \overline{57}$, $\overline{6}^{-1} \equiv \overline{12}$.
   (f) Units are $\{1, 3, 5, 9, 11, 13\}$, zero divisors are $\{2, 4, 6, 7, 8, 10, 12\}$.
   (g) Cancel 5 to get $n \equiv 24 \pmod{38}$.
   (h) Cancel 2 to get $3n \equiv 5 \pmod{50}$, then multiply by $3^{-1} \equiv 17$ to get $n \equiv 35 \pmod{50}$.
   (i) Plug in $n = 3 + 20a$ to $n \equiv 4 \pmod{19}$ to get $n \equiv 23 \pmod{380}$.
   (j) Plug in $n = 7 + 14a$ to $n \equiv 2 \pmod{9}$ to get $n \equiv 119 \pmod{126}$.
   (k) Since 11 is prime, we have $10! \equiv -1 \pmod{11}$ by Wilson's theorem.
   (l) Since 47 is prime, we have $2^{47} \equiv 2 \pmod{47}$ by Fermat's little theorem.
   (m) Since $\varphi(25) = 20$, we have $6^{20} \equiv 1 \pmod{25}$ by Euler's theorem.
   (n) $\varphi(121) = \varphi(11^2) = (11^2 - 11) = 110$ and $\varphi(5^5 7^{10}) = (5^5 - 5^4)(7^{10} - 7^9)$.
   (o) 3 or 5, since they are the only elements with order 6 modulo 7.
   (p) If $x = 0.1\overline{25}$ then $990x = 1000x - 10x = 125.\overline{25} - 1.\overline{25} = 124$, so $x = 124/990$.
   (q) 10 has order 2 mod 11, so 7/11 has period 2.

---

5. Here are brief responses:

   (a) The Caesar shift is insecure: it can be broken very easily by hand as it has only 26 possible decodings.
   (b) 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.
   (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.
   (d) Using a zero-knowledge protocol like the Rabin protocol described in class, where Peggy proves to an arbitrarily high probability that she knows the square root of a particular value s^2 modulo $N = pq$, will allow Peggy to convince Victor that she knows the secret s without revealing any information that makes s easily calculable.
   (e) Using primality/compositeness tests like the Fermat test, the Lucas primality criterion, or Miller-Rabin, allow for rapid and accurate testing of primality even for very large integers.
   (f) Among the various factorization algorithms discussed in class like trial division, Pollard $p-1$, Pollard ρ, and the sieving methods, none allows for extremely fast factorization of large integers (factoring integers more than 100 base-10 digits takes a huge amount of time and memory).

---

6. Here are brief outlines of each proof:

   (a) Induct on n. Base case $n = 1$ has $F_1 + F_3 = 3 = F_4$. 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 case $n = 1$ clear. 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.
   (c) Note $p|a \cdot a$, so since p is prime then $p|a$ or $p|a$. Since the two conclusion statements are the same, we have $p|a$.
   (d) If p is prime and $p|k^2$ and $p|(k+1)^2$ then by (b) we have $p|k$ and $p|(k+1)$ so that $p|(k+1) - k = 1$, impossible.
   (e) Suppose $xy = 0$. Then $(ux)y = u(xy) = u0 = 0$, and also $ux \neq 0$ since if $ux = 0$ then $x = u^{-1}(ux) = 0$, contradiction. So ux is a zero divisor.
   (f) 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 order does not divide 2 or 3, hence must be 6.
   (g) Induct on n. Base case $n = 1$. Inductive step: if $b_n = 2^n + n$ then $b_{n+1} = 2(2^n + n) - n + 1 = 2^{n+1} + (n+1)$.
   (h) Induct on n. Base case $n = 1$: $\frac{1}{2} = \frac{1}{2}$. Inductive step: if $\frac{1}{1\cdot 2} + \frac{1}{2\cdot 3} + \frac{1}{3\cdot 4} + \cdots + \frac{1}{n\cdot(n+1)} = \frac{n}{n+1}$ then $\frac{1}{1\cdot 2} + \frac{1}{2\cdot 3} + \frac{1}{3\cdot 4} + \cdots + \frac{1}{n\cdot(n+1)} + \frac{1}{(n+1)\cdot(n+2)} = \frac{n}{n+1} + \frac{1}{(n+1)\cdot(n+2)} = \frac{n+1}{n+2}$ as required.
   (i) Note $4^{239} \equiv 4 \pmod{239}$ by Fermat, so $4^{240} \equiv 4 \cdot 4 \equiv 16 \pmod{239}$. Likewise, since $\varphi(55) = 40$, $4^{40} \equiv 1 \pmod{55}$ by Euler, so $2^{240} \equiv (2^{40})^6 \equiv 1^6 \equiv 1 \pmod{55}$.
   (j) By Euler, $a^4 \equiv 1 \pmod 5$ for every unit, and $0^4 \equiv 0 \pmod 5$. Then the sum of three fourth powers is 0, 1, 2, or 3 mod 5, hence cannot be 2024 since 2024 is 4 mod 5.
   (k) 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.
   (l) Induct on n with base cases $n = 1$ and $n = 2$. 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.
   (m) If $a = b$ then $\gcd(a, a) = a = \operatorname{lcm}(a, a)$. Conversely if $\gcd(a, b) = \operatorname{lcm}(a, b)$ 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 $a = b$.
   (n) Note $3^1 \equiv 3$, $3^2 \equiv 9$, $3^4 \equiv 81 \equiv 20$, $3^8 \equiv 400 \equiv 34$. So $3^{10} \equiv 3^8 \cdot 3^2 \equiv 34 \cdot 9 \equiv 1$ so the order divides 10. But $3^5 \equiv 3^4 \cdot 3 \equiv 60$ and $3^2 \equiv 9$, so the order does not divide 2 or 5, so it is 10.
   (o) 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 $99! - 1$.
   (p) Note $\gcd(n, n+p) = \gcd(n, p)$ by gcd properties. Then $\gcd(n, p)$ divides p so is either 1 or p, and it is equal to p if and only if $p|n$ (by definition of gcd).
   (q) Induct on n. Base cases $n = 1$ and $n = 2$ have $c_1 = 2^{F_1}$ and $c_2 = 2^{F_2}$. Inductive step: if $c_n = 2^{F_n}$ and $c_{n-1} = 2^{F_{n-1}}$ then $c_{n+1} = c_n c_{n-1} = 2^{F_n} 2^{F_{n-1}} = 2^{F_n + F_{n-1}} = 2^{F_{n+1}}$.
   (r) Let p be prime. If p divides a, b then p^2 divides a^2, b^2. Conversely if p divides a^2, b^2 then p divides a, b by (b).
