1. You are highly encouraged to write up 1 or 2 sentences on each of these topics yourself.

2. This problem is from homework 1. Please review the Euclidean algorithm there and in the notes if you had trouble. The answers are (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) $1 = -55 \cdot 233 + 89 \cdot 144$.

3. (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.

4. 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.

5. (a) By Euclid, gcd 8, lcm $256 \cdot 520/8$. (b) By Euclid, gcd 3, lcm $921 \cdot 177/3$. (c) gcd $2^3 3^2 5^4$, lcm $2^4 3^3 5^4 7 \cdot 11$.
(d) sum is $\overline{2}$, difference is $\overline{6}$, product is $\overline{0}$. (e) $\overline{4}^{-1} \equiv \overline{18}$, $\overline{5}^{-1} \equiv \overline{57}$, $\overline{6}^{-1} \equiv \overline{12}$.
(f) Units $\{1,3,5,9,11,13\}$, zero divs $\{2,4,6,7,8,10,12\}$. (g) $n \equiv 24 \pmod{38}$ (h) $n \equiv 35 \pmod{50}$
(i) $n \equiv 23 \pmod{380}$. (j) $n \equiv 119 \pmod{126}$. (k) $10 \equiv -1$ by Wilson's theorem (l) 2 by Fermat's little theorem
(m) 1 by Euler's theorem (n) $\varphi(121) = 110$ and $\varphi(5^5 7^{10}) = 5^4 4 \cdot 7^9 6$. (o) 3 or 5
(p) $\varphi(\varphi(97)) = \varphi(96) = 32$. (q) 124/990 (r) 10 has order 2 mod 11, so period 2.

6. (a) Induct on n with base case $n = 1$. 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.
(b) 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 $p|a$.
(c) Suppose $xy = 0$. Then $(ux)y = u(xy) = u0 = 0$, and also $ux \neq 0$ since multiplying by u^{-1} would give $x = 0$ (impossible). So ux is also a zero divisor.
(d) 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.
(e) Induct on n. Base case $n = 1$. Inductive step: if $b_n = 2^n + n$ then $b_{n+1} = 2(2^n + n) - n + 1 = 2^{n+1} + (n+1)$.
(f) If $p | k^2$ and $p | (k+1)^2$ then by (b) we have $p | k$ and $p | (k+1)$ so that $p | (k+1) - k = 1$, impossible. Alternatively, could use Euclid to see that $(2k+3)k^2 - (2k-1)(k+1)^2 = 1$.
(g) 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.
(h) 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 $2^{240} \equiv (2^{40})^6 \equiv 1^6 \equiv 1 \pmod{55}$.
(i) 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.
(j) 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.
(k) 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.
(l) 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 $a = b$.
(m) 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.
(n) 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 $99! - 1$.