No calculators are allowed. You may reference and use any results that were stated in class, unless you are explicitly asked to prove it. When you do use them, please state clearly which result you are using.

For Math 346 students, the problem with the lowest score will be dropped. The bonus problem will count as extra credit for everyone.

(1) (3+5+2 points)
(a) An element $g$ is a primitive root if $\text{ord}_n(g) = \phi(n)$. That is, $g$ generates $U(\mathbb{Z}/n\mathbb{Z})$.
(b) Since $\phi(29) = 28 = 2^2 \cdot 7$, so we need to check that $2^{14} \not\equiv 1 \pmod{29}$ and also that $2^4 \not\equiv 1 \pmod{29}$. First, $2^4 = 16 \not\equiv 1 \pmod{29}$. Now, $2^{14} = 2^5 \cdot 2^5 \cdot 2^4 \equiv 3 \cdot 3 \cdot 16 \equiv 144 \equiv -1 \pmod{29}$, so 2 is a primitive root.
(c) $U(\mathbb{Z}/29\mathbb{Z})$ must be a cyclic group of order 28, because 2 is a primitive root.

(2) (6+4 points)
(a) Wilson’s theorem states that $(p - 1)! \equiv -1 \pmod{p}$, where $p$ is a prime. We consider the group $U(\mathbb{Z}/p\mathbb{Z}) = \{1, 2, \ldots, p - 1\}$. Since all of these elements have inverses, we can pair up the elements with their inverses, except for 1 and $p - 1$, which satisfy the equation $x^2 \equiv 1 \pmod{p}$, and so are their own inverses. Thus, multiplying all of the elements in $U(\mathbb{Z}/p\mathbb{Z})$ together, most of them cancel against their inverses, except for $p - 1$. That is, $(p - 1)! \equiv p - 1 \equiv -1 \pmod{p}$.
(b) If $n$ is not a prime, we can write $n = ab$. Unless $n = p^2$, we can write $n$ so that $a \neq b$, with $a, b \leq n - 1$. In particular, this means that $ab|(n - 1)!$, that is, $(n - 1)! \equiv 0 \pmod{n}$ for $n \neq p^2$. If $n = p^2$ for some prime $p \geq 3$, then $n - 1 = p^2 - 1 > 2p$, so $(n - 1)!$ includes at least two copies of $p$. That is, $(n - 1)! \equiv 0 \pmod{n}$. If $p = 2$, however, we see that $(2 - 1)! = 1 \not\equiv 0 \pmod{4}$.

(3) (10 points) If we could show that $ab(a^2 - b^2)(a^2 + b^2) \equiv 0 \pmod{2}$, then we would be done by Chinese remainder theorem. To show that 2 divides $ab(a^2 - b^2)(a^2 + b^2)$, note that if either $a$ or $b$ were even, then we are done. If $a$ and $b$ are both odd, then $a + b$ is even, and $a + b|a^2 - b^2$. Now we show that 3 divides $ab(a^2 - b^2)(a^2 + b^2)$. Again, if 3|a or 3|b, then we are done, so assume that 3 \n| a, b. Write $a = 3a' + r$ with $r = 1, 2$. Then $a^2 = 9a'^2 + 6a'r + r^2 \equiv 1 \pmod{3}$, so if 3 \n| a, b, then $a^2, b^2 \equiv 1 \pmod{3}$, so 3|a^2 - b^2. Similarly, if 5 \n| a, b, then $a^2, b^2 \equiv 1, 4 \pmod{5}$, so one of $a^2 - b^2$ or $a^2 + b^2$ must be divisible by 5 (depending on whether $a^2 \equiv b^2 \pmod{5}$ or $a^2 \not\equiv b^2 \pmod{5}$, respectively).

(4) (10 points) Since $\gcd(u, v) = 1$, there exist $a, b \in \mathbb{Z}$ such that $au + bv = 1$. Now, $2 = 2au + 2bv = a[(u+v)+(u-v)] + b[(u+v)-(u-v)] = (a+b)(u+v) + (a-b)(u-v)$, so $2 \in (u+v, u-v)$. The only ideals of $\mathbb{Z}$ that contain 2 are (1) and (2), so $\gcd(u+v, u-v) = 1$ or 2.
(5) \( \text{ord}_p(a) = 3 \) implies that \( a^3 \equiv 1 \mod p \). That is, \( a^3 - 1 = (a - 1)(a^2 + a + 1) \mod p \). We must have \( a - 1 \not\equiv 0 \mod p \) because otherwise \( \text{ord}_p(a) = 1 \), so we have \( a^2 + a + 1 \equiv 0 \mod p \). Now, using this identity, we have

\[
(a + 1)^6 = a^6 + 6a^5 + 15a^4 + 20a^3 + 15a^2 + 6a + 1
\equiv a^4(a^2 + a + 1) + 5a^5 + 14a^4 + 20a^3 + 15a^2 + 61 + 1
\equiv 5a^5 + 14a^4 + 20a^3 + 15a^2 + 6a + 1
\equiv 5a^3(a^2 + a + 1) + 9a^4 + 15a^3 + 15a^2 + 6a + 1
\equiv 9a^2(a^2 + a + 1) + 6a(a^2 + a + 1) + 1 \equiv 1 \mod p
\]

so \( \text{ord}_p(a + 1) | 6 \). Now we need to show that \( \text{ord}_p(a + 1) \neq 2, 3 \). We have \( (a + 1)^2 \equiv a \mod p \), so \( \text{ord}_p(a + 1) \neq 2 \) unless \( a = 1 \). But then \( \text{ord}_p(a) = 1 \), so \( a \neq 1 \) and \( \text{ord}_p(a + 1) \neq 2 \). Similarly, \( (a + 1)^3 = a^3 + 3a^2 + 3a + 1 \equiv 2a^2 + 2a + 1 \equiv -1 \mod p \), so \( \text{ord}_p(a + 1) \neq 3 \). Thus, \( \text{ord}_p(a + 1) = 6 \).

**Bonus. (3 points)** Suppose that we had \( \sqrt{3} + \sqrt{7} = \frac{a}{b} \) for \( a, b \in \mathbb{Z}, b \neq 0 \). Then \( 3 = (\frac{a}{b} - \sqrt{7})^2 = \frac{a^2}{b^2} - 2\sqrt{7}\frac{a}{b} + 7 \). Multiplying by \( b^2 \) and squaring again gives \( a^4 - 20a^2b^2 + 16b^4 = 0 \). But it can be checked through various means that this equation does not have any integral solutions (for example, use the quadratic formula, etc.)