E. Dummit's Math 3527 ~ Number Theory I, Spring 2026 ~ Midterm 2 Solutions (Form M)

---

1. Each item was worth 3 points.

   (a) $\boxed{\text{True}}$: a test like the Fermat test, Miller-Rabin test, or the AKS primality test can prove that a large integer is composite without finding a factorization.

   (b) $\boxed{\text{False}}$: using Pollard's ρ-algorithm or one of the sieving methods on a modern computer allows us to factor integers up to 90 digits very quickly. (Mathematica factors $2^{101}-1$ in 1.60 milliseconds.)

   (c) $\boxed{\text{False}}$: a polynomial of degree 4 or higher with no roots could still be the product of two irreducible quadratics. For example, in $\mathbb{R}[x]$, the polynomial $p(x) = x^4 + 5x^2 + 4$ has no roots, but it nonetheless factors as $(x^2+1)(x^2+4)$.

   (d) $\boxed{\text{False}}$: as proven in class, there is a primitive root mod m only when $m = 1$, 2, 4, p^d, or $2p^d$ for an odd prime p, so for instance there is no primitive root modulo 8.

---

2. Item (a) was worth 2 points while the others were worth 3 points.

   (a) Since $307^2 - N = 900 = 30^2$ we see $N = 307^2 - 30^2 = (307-30)(307+30) = \boxed{277 \cdot 337}$.

   (b) Note that $N(5-2\sqrt{6}) = (5-2\sqrt{6})(5+2\sqrt{6}) = 5^2 - 2^2 \cdot 6 = 1$. Thus, the inverse of $5-2\sqrt{6}$ is its conjugate $\boxed{5+2\sqrt{6}}$.

   (c) We take the lower power of each irreducible factor for the gcd, so the gcd is $\boxed{x^3(x-2)^2}$.

   (d) By the formula proven in class, the number of monic irreducible polynomials of degree 3 modulo p is $(p^3-p)/3$. With $p=5$ this evaluates to $(5^3-5)/3 = \boxed{40}$.

   (e) The first congruence has solution $p = 2+(x-2)q$. Plugging into the second congruence yields $2+(x-2)q \equiv 6 \pmod{x-4}$ which since $x-2 \equiv 2 \pmod{x-4}$ reduces to $2q \equiv 4 \pmod{x-4}$ so that $q \equiv 2 \pmod{x-4}$. Then $q = 2+(x-4)r$, and so $p = 2+(x-2)q = 2x-2+(x-2)(x-4)r$. The solution is $p \equiv \boxed{2x-2 \pmod{x^2-6x+8}}$.

---

3. Each part was worth 5 points.

   (a) We use the Euclidean algorithm. Since $\dfrac{3+5i}{2+4i} = \dfrac{(3+5i)(2-4i)}{(2+4i)(2-4i)} = \dfrac{26-2i}{20} = 1.3 - 0.1i$, rounding to the nearest Gaussian integer yields quotient $q = 1$ and thus remainder $r = (3+5i)-(2+4i) = 1+i$. Then $\dfrac{2+4i}{1+i} = \dfrac{(2+4i)(1-i)}{(1+i)(1-i)} = \dfrac{6+2i}{2} = 3+i$ so the quotient is $3+i$ with remainder 0. The gcd is the last nonzero remainder $\boxed{1+i}$.

   (b) We use the Euclidean algorithm again. Since $\dfrac{3+5i}{2-i} = \dfrac{(3+5i)(2+i)}{(2-i)(2+i)} = \dfrac{1+13i}{5} = 0.2+2.6i$, rounding to the nearest Gaussian integer yields quotient $q = 3i$ and thus remainder $r = (3+5i)-3i(2-i) = -i$. Then $\dfrac{2-i}{-i} = 1+2i$ with remainder 0. Solving for the last nonzero remainder yields $-i = (3+5i)-3i(2-i)$. Scaling both sides by $(-i)^{-1} = i$ yields $1 = i(3+5i)+3(2-i)$, and finally reducing mod $3+5i$ yields $3(2-i) \equiv 1 \pmod{3+5i}$. Hence the inverse of $2-i$ is $\boxed{3}$.

---

4. Part (a) was worth 2 points, the tables were 2 ($+$) and 4 ($\cdot$) points, (c) was 3 points, and (d) was 3 points.

   (a) Since $p(2) = 0$ factoring yields $p = \boxed{(x-2)^2 = (x+1)^2}$.

   (b) Since $x^2 + x + 1 \equiv 0$ we have $x^2 \equiv -2x - 1 \equiv x + 2$. Using this and reducing the coefficients mod 3 we get the following:

$+$	$\overline{x}$	$\overline{x+1}$	$\overline{x+2}$
$\overline{x}$	$\overline{2x}$	$\overline{2x+1}$	$\overline{2x+2}$
$\overline{x+1}$	$\overline{2x+1}$	$\overline{2x+2}$	$\overline{2x}$
$\overline{x+2}$	$\overline{2x+2}$	$\overline{2x}$	$\overline{2x+1}$

$\cdot$	$\overline{x}$	$\overline{x+1}$	$\overline{x+2}$
$\overline{x}$	$\overline{x+2}$	$\overline{2x+2}$	$\overline{2}$
$\overline{x+1}$	$\overline{2x+2}$	$\overline{0}$	$\overline{x+1}$
$\overline{x+2}$	$\overline{2}$	$\overline{x+1}$	$\overline{2x}$

   (c) The units are the residue classes that are relatively prime to $p = (x+1)^2$ while the zero divisors are the residue classes that are not relatively prime (which are just the multiples of $x+1$). So the units are $\boxed{1, 2, x, x+2, 2x, 2x+1}$ while the zero divisors are $\boxed{x+1, 2x+2}$.

   (d) Since there are 6 units as noted in (c), we compute $\overline{x+2}^6$. From (b) we see $\overline{x+2}^2 = \overline{2x}$ and then $\overline{x+2}^3 = \overline{x+2}^2\overline{x+2} = 2\overline{x(x+2)} = \overline{1}$ and so $\overline{x+2}^6 = \overline{1}$ also.

---

5. Part (a) was worth 2 points, (b) and (c) were each worth 4 points, and (d) was worth 2 points.

   (a) If $a^2 + 6b^2 = 2$ or 5 then we must have $b = 0$ since $6b^2$ is too large otherwise, but $a^2 = 2$ or 5 has no integer solution for a.

   (b) If $2 + \sqrt{-6} = rs$ for some r, s, then taking norms yields $10 = N(2+\sqrt{-6}) = N(rs) = N(r)N(s)$. Since the norms are positive, the only possibilities for $N(r)$ are 1, 2, 5, 10. But by (a) there are no elements of norm 2 or 5, so either $N(r) = 1$ or $N(r) = 10$ in which case $N(s) = 1$: then r or s is a unit. By definition, $2 + \sqrt{-6}$ is irreducible.

   (c) Note that $(2+\sqrt{-6})(2-\sqrt{-6}) = 10$ so $2 + \sqrt{-6}$ divides the product $2 \cdot 5$. However, $2 + \sqrt{-6}$ does not divide 2 or 6, since $\dfrac{2}{2+\sqrt{-6}} = \dfrac{2-\sqrt{-6}}{5}$ and $\dfrac{5}{2+\sqrt{-6}} = \dfrac{2-\sqrt{-6}}{2}$, and neither of these has integer coefficients. This means $2 + \sqrt{-6}$ is not prime.

   (d) In a Euclidean domain, irreducible elements are prime. Since $2 + \sqrt{-6}$ is irreducible but not prime, R cannot be Euclidean.

---

6. As shown in class, $F[x]$ modulo q is a field if and only if q is irreducible. Here, since $q = x^2 + x + 4$ has degree 2, to show it is irreducible we only have to show that q has no roots modulo 7. We compute $q(0) = 4$, $q(1) = 6$, $q(2) = 10 = 3$, $q(3) = 16 = 2$, $q(4) = 24 = 3$, $q(5) = 34 = 6$, and $q(6) = 46 = 4$: since none of these is zero, q has no roots, hence is irreducible, so $\mathbb{F}_7[x]$ modulo q is a field. The residue classes are of the form $\overline{ax+b}$ for $a, b \in \mathbb{F}_7$ so there are indeed exactly $7 \cdot 7 = 49$ elements.

---

7. Part (a) was worth 5 points, (b) was worth 2 points, and (c) was worth 3 points.

   (a) First, 7 is a primitive root mod 13: we have $7^{12} \equiv 1 \pmod{13}$ by Euler's theorem, but $7^4 \equiv 9$ and $7^6 \equiv 7^4 7^2 \equiv 9 \cdot 10 \equiv -1 \bmod 13$, so the order divides 12 but not 4 or 6 hence is 12. Also, we are given $7^{12} \not\equiv 1 \pmod{13^2}$, and as shown in class since 7 is a primitive root mod 13 this implies it is also a primitive root mod 13^2.

   (b) As proven in class, a primitive root mod p^d is also a primitive root mod all higher powers of p, so $\boxed{7}$ is a primitive root mod 13^{2026}.

   (c) The number of primitive roots is $\varphi(\varphi(13^{2026})) = \varphi(12 \cdot 13^{2025}) = \boxed{48 \cdot 13^{2024}}$.
