E. Dummit's Math 3527 ~ Number Theory 1, Spring 2024 ~ Midterm 2 Review Answers

---

1. Note that depending on your calculations, you may end up with an associate of the listed answer, which would also be correct.

   (a) GCD is $x^2 + x$, with linear combination $1 \cdot (x^4 + x) + x \cdot (x^3 + x) = x^2 + x$.

   (b) GCD is $4 + i$, with linear combination $-1 \cdot (11 + 24i) + (1 + 2i)(13 - i) = 4 + i$.

   (c) GCD is $x - 1$, with linear combination $\frac{1}{6}(x^3 - x) - \frac{1}{6}(x + 3)(x^2 - 3x + 2) = x - 1$.

   (d) GCD is 1, with linear combination $(1 - 2i)(9 - 5i) + (4 + 5i)(3 + 2i) = 1$.

---

2. Note that $\overline{a}$ is a unit precisely when a, p are relatively prime (and we can compute the inverse x of a using the Euclidean algorithm to find x, y with $xa + yp = 1$ yielding $xa \equiv 1 \bmod p$), while $\overline{a}$ is a zero divisor when a, p are not relatively prime (in which case $b = p/\gcd(a, p)$ has $ab \equiv 0 \bmod p$).

   (a) Zero divisor since gcd is $2 - i$, have $(2 - i) \cdot (1 + 3i) = 0 \bmod p$.

   (b) Unit since gcd is 1, have $\frac{1}{7}(-x + 3)(x + 3) + \frac{1}{7}(x^2 - 2) = 1$ so inverse is $\frac{1}{7}(-x + 3)$.

   (c) Unit since gcd is 1, have $(1 + 4i)(3 + 4i) + 2(7 - 8i) = 1$ so inverse is $1 + 4i$.

   (d) Zero divisor since gcd is $x + 1$, have $(x^2 + x) \cdot (x^3 + x^2 + x + 1) = 0 \bmod p$.

   (e) Unit since gcd is 1, have $(2x^2 + 2x + 4)(x^2 + x) + (3x + 1)(x^3 + 3x + 1) = 1$ so inverse is $2x^2 + 2x + 4$.

---

3. (a) Need $a^2 + 2b^2 = 9$ yielding ± 3 and $\pm 1 \pm 2\sqrt{-2}$.

   (b) Quotient 5, remainder $-1 - 2i$.

   (c) Quotient $x^2 - 1$, remainder x.

   (d) Inverse of $1 + i$ is $-4 + 3i$ so solution is $n \equiv 3(-4 + 3i) \pmod{8 + i}$.

   (e) Solution is $z \equiv 2 + 9i \pmod{7 + 19i}$.

   (f) Solution is $p \equiv x + 2x^2 \pmod{x^3 - 2x^2}$.

   (g) The classes are represented by polynomials of degree ≤ 2, so there are 7^3 residue classes.

   (h) Units are $\overline{1}$, $\overline{2}$ $\overline{x + 1}$, $\overline{2x + 2}$; zero divisors are $\overline{x}$, $\overline{x + 2}$, $\overline{2x}$, $\overline{2x + 1}$.

   (i) Units are $\overline{ax + b}$ where $b \neq 0$ (20 total); zero divisors are $\overline{x}$, $\overline{2x}$, $\overline{3x}$, $\overline{4x}$.

   (j) Searching for roots produces factorizations $x(x+1)$, $(x + 1)^2$, and $(x + 2)^2$.

   (k) Total is $\frac{1}{7}(2^7 - 2) = 18$.

   (l) Total is $\frac{1}{4}(7^4 - 7^2) = 588$.

   (m) Total is $\frac{1}{10}(2^{10} - 2^5 - 2^2 + 2^1) = 99$.

   (n) There are primitive roots mod 34 and 37 but not mod 35 or mod 36.

   (o) 2 is a primitive root mod 3^2 hence mod 3^{2024}. Total number is $\varphi(\varphi(3^{2024})) = 2 \cdot 3^{2022}$.

   (p) 2 is a prim root mod 3^{2024} so $2 + 3^{2024}$ is a prim root mod $2 \cdot 3^{2024}$. Total number is $\varphi(\varphi(2 \cdot 3^{2024})) = 2 \cdot 3^{2022}$.

   (q) The number of residue classes is $N(7 - 5i) = 49 + 25 = 74$.

   (r) By drawing the fundamental region (square with vertices 0, β, $i\beta$, $(1+i)\beta = 0$, $2-i$, $1+2i$, $3+i$), and picking inequivalent points, we get 0, 1, 2, $1 + i$, $2 + i$.

   (s) $5 + 5i = (1 + i)(2 + i)(2 - i)$, up to associates.

   (t) $11 + 12i = i(2 - i)(7 - 2i)$, up to associates.

   (u) $999 = 3^3(6 - i)(6 + i)$, up to associates.

---

4. (a) The residue classes are represented by polynomials of degree less than 3: $\overline{0}, \overline{1}, \overline{x}, \overline{x + 1}, \overline{x^2}, \overline{x^2 + 1}, \overline{x^2 + x}, \overline{x^2 + x + 1}$.

   (b) We have $\overline{x^2} + \overline{x^2 + 1} = \overline{1}$, $\overline{x^2} \cdot \overline{x^2 + 1} = \overline{x^2 + 1}$, and $\overline{x^2 + 1}^2 = \overline{0}$.

   (c) The units are the polynomials relatively prime to the modulus: $\overline{1}, \overline{x}, \overline{x^2}, \overline{x^2 + x + 1}$.
   The zero divisors are the nonzero polynomials not relatively prime to the modulus: $\overline{x + 1}$, $\overline{x^2 + 1}$, $\overline{x^2 + x}$.

   (d) There are 4 units and indeed $\overline{x^2 + x + 1}^4 = \overline{x^2}^2 = \overline{1}$ as required.

   (e) Multiply by the inverse of $\overline{x^2}$, which is $\overline{x^2}$ again, to see $q(x) \equiv x^2(x + 1) \equiv x + 1$.

---

5. Here are brief responses:

   (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) 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).

   (d) Trial division will be very slow for 40-digit integers, but Pollard ρ and the sieving methods will allow us to factors of that size quite rapidly (Pollard ρ typically 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).

---

6. Many problems of similar types were covered on at least one homework.

   (a) Note $N(7+4\sqrt{3}) = 1$ so it is a unit since the norm is ± 1. The inverse is the conjugate $7 - 4\sqrt{3}$.

   (b) Note $N[(1+\sqrt{5})^{2023}] = N(1+\sqrt{5})^{2023} = (-4)^{2023}$ so it is not a unit. But $N[(2+\sqrt{5})^{2023}] = N(2+\sqrt{5})^{2023} = (-1)^{2023} = -1$ so it is a unit.

   (c) Note $N(4+5i) = 4^2 + 5^2 = 41$ is a prime integer so as $\mathbb{Z}[i]$ is Euclidean, $4+5i$ is irreducible and prime.

   (d) Note $N(2+\sqrt{-7}) = 11$ is a prime integer, so $2+\sqrt{-7}$ is irreducible.

   (e) Note $N(1+\sqrt{-7}) = 8$ so if we had a nontrivial factorization, it would have to be the product of an element of norm 2 with an element of norm 4. But since $N(a+b\sqrt{-7}) = a^2 + 7b^2$ there are no elements of norm 2 or 4, so there is no possible factorization.

   (f) Note that $(1+\sqrt{-7})(1-\sqrt{-7}) = 8 = 2 \cdot 4$ so $1+\sqrt{-7}$ divides $2 \cdot 4$ but it divides neither 2 nor 4, since $2/(1+\sqrt{-7}) = (1-\sqrt{-7})/4$ and $4/(1+\sqrt{-7}) = (1-\sqrt{-7})/2$. This means $1+\sqrt{-7}$ is not prime.

   (g) x^2+x+1 has no roots in $\mathbb{F}_2$ by a direct check, so since it has degree 2, it is irreducible hence also prime since $F[x]$ is Euclidean.

   (h) It is not hard to list all the units to see that there are 4 of them (they are the polynomials with constant term 1). We then calculate $\overline{x^2+1}^4 = \overline{x^4+2x^2+1}^2 = \overline{1}^2 = \overline{1}$ so Euler's theorem holds.

   (i) There are $N(3+2i) = 13$ residue classes and $i^{13} \equiv i \pmod{3+2i}$ as required (indeed, i^{13} just equals i).

   (j) For $p(x) = x^3+x+1$ we have $p(0) = p(2) = p(3) = 1$, $p(1) = 3$, $p(4) = 4$ mod 5, so p has no roots. Since it has degree 3 it is irreducible, so $\mathbb{F}_5[x]$ modulo x^3+x+1 is a field.

   (k) Searching yields a root $x = 3$, so the polynomial is reducible so $\mathbb{F}_5[x]$ modulo x^4+x+1 is not a field.

   (l) Note that x^2+2x+8 has no real roots (its roots are $-1 \pm i\sqrt{7}$). Since it has degree 2 it is irreducible, so $\mathbb{R}[x]$ modulo x^2+2x+8 is a field.

   (m) Since $125 = 5^3$ we can use $\mathbb{F}_5[x]$ modulo an irreducible polynomial of degree 3. We actually just identified such a polynomial, namely x^3+x+1, in part (j).

   (n) There are $N(4+i) = 17$ residue classes hence 16 units since $4+i$ is irreducible. Then $(1+i)^2 \equiv 2i$, so $(1+i)^4 \equiv (2i)^2 \equiv -4 \equiv i$, $(1+i)^8 \equiv i^2 \equiv -1$, and finally $(1+i)^{16} \equiv (-1)^2 \equiv 1$ as required.
