E. Dummit's Math 3527 $\sim$ Number Theory 1, Spring 2022 $\sim$ Midterm 2 Review Answers

---

1. These topics were all discussed in the cryptography chapter of the notes and during the lectures.

   (a) False: most historical cryptosystems were not particularly secure and are fairly easy to break (Caesar shift, substitution ciphers, etc.). Only in the 20th century were provably secure cryptosystems actually implemented.

   (b) False: there exist secure symmetric cryptosystems just as there are secure asymmetric cryptosystems.

   (c) False: although Rabin encryption should not be used, that isn't because Rabin is insecure (it isn't, if implemented properly and decrypted messages are never revealed), but rather that there exists an attack that can break Rabin if Eve has access to Bob's decryption program.

   (d) True (or at least as far as we know): RSA encryption is used in the present day to secure internet traffic.

   (e) True: Peggy could use a zero-knowledge system like the one discussed in class modeled after Rabin encryption.

   (f) True: there are numerous fast primality/compositeness tests like Miller-Rabin and the AKS primality test.

   (g) False: even if an integer passes the Fermat test, it need not be prime, as it could be a Carmichael number like 561.

   (h) False (or at least as far as we know): factorization seems to be much harder than primality testing, and factoring things like 500-digit numbers seems totally out of reach with current technology.

---

2. This problem is very similar to problem 2 from homework 7. Note that depending on your calculations, you may end up with an associate of the listed answer (which would also be correct). We list the monic GCD for polynomials and the GCD $a+bi$ with $a > |b|$ for Gaussian integers.

   (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 $\dfrac{1}{6}(x^3-x) - \dfrac{1}{6}(x+3)(x^2-3x+2) = x-1$.

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

---

3. This problem is very similar to problem 1 from homework 9. 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 $xa + ya \equiv 1 \bmod p$), 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 $2x^2+2x+4$.

---

4. This problem is similar to problems 2 and 3 from homework 8.

   (a) The residue classes are $\overline{0}, \overline{1}, \overline{x}, \overline{x+1}, \overline{x^2}, \overline{x^2+1}, \overline{x^2+x}, \overline{x^2+x+1}$.

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

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

(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 $q(x) \equiv x^2(x+1) \equiv x^2+1$.

---

5. Most of these problem types were covered on at least one homework (and in most cases, also the lecture notes or slides).

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

---

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 $N[(1+\sqrt{5})^{2022}] = N(1+\sqrt{5})^{2022} = (-4)^{2022}$ so it is not a unit. But $N[(2+\sqrt{5})^{2022}] = N(2+\sqrt{5})^{2022} = (-1)^{2022} = 1$ so it is a unit.

(c) Note $N(4 + 5i) = 4^2 + 5^2 = 41$ is a prime integer, so since $\mathbb{Z}[i]$ 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) We have $i^5 \equiv i \pmod{2 + i}$ as required. Indeed, i^5 actually 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 not irreducible. Thus, $\mathbb{F}_5[x]$ 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).
