SPRING 2025: MATH 540 EXAM 2

You must provide all details to receive full credit. You may use calculators on this exam. Please put your name on all pages that you turn in.

Name:

Statements. Define any terms you use in the statements below. (3 points each)

1. State the Chinese Remainder Theorem.

Solution. Suppose $n_1, \ldots, n_r \in \mathbb{Z}$ are positive integers such that for all $i \neq j$, $\gcd(n_i, n_j) = 1$. Then for all $a_1, \ldots, a_r \in \mathbb{Z}$, the system of congruences

$$\begin{aligned} x &\equiv a_1 \bmod n_1 \\ x &\equiv a_2 \bmod n_2 \\ &\vdots \\ x &\equiv a_r \bmod n_r \end{aligned}$$

has a solution in $\mathbb{Z}$. Moreover, if x, y are solutions to the system, then $x \equiv y \bmod N$, where $N = n_1 \cdot n_2 \cdots n_r$.

2. State the Division Algorithm for Gaussian integers.

Solution. Let u, v be Gaussian integers, then there exist Gaussian integers q, r with $r = 0$, or $N(r) < N(v)$, such that $u = vq + r$.

3. State Gauss's Lemma related to quadratic reciprocity.

Solution. Let p be an odd prime and $a \in \mathbb{Z}$ not divisible by p. Consider the list of positive integers $L := \{a, 2a, 3a, \ldots, \frac{p-1}{2} \cdot a\}$. For each $1 \leq k \leq \frac{p-1}{2}$, take n_k in the open interval $(-\frac{p}{2}, \frac{p}{2})$ such that $n_k \equiv ka \bmod p$. If v is the number of negative n_k, then $(\frac{a}{p}) = (-1)^v$.

4. State the Quadratic reciprocity Theorem.

Solution. For odd primes $p \neq q$, $(\frac{p}{q}) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} (\frac{q}{p})$.

If p is an odd prime, then $(\frac{2}{p}) = \begin{cases} 1, \text{ if } p \equiv 1, 7 \bmod 8 \\ -1 \text{ if } p \equiv 3, 5 \bmod 8 \end{cases}$.

5. Define what it means to be a primitive root of one mod p, for p an odd prime.

Solution. Given integers a, n with $\mathrm{GCD}(a, n) = 1$, the order of a mod n is the least positive integer r such that $a^r \equiv 1 \bmod n$. The integer a is a primitive root of 1 mod p if its order mod p is $p - 1$.

Calculations (10 points each)

1. Solve the following system of congruences: $3x \equiv 4 \pmod{5}$, $x \equiv 2 \pmod{8}$, $2x \equiv 7 \pmod{11}$.

Solution. Removing the coefficients of x in the given system of congruences, we must solve: $x \equiv 3 \bmod 5$, $x \equiv 2 \bmod 8$, $x \equiv 9 \bmod 11$. Next we take $N = 5 \cdot 8 \cdot 11 = 440$, $N_1 = \frac{440}{3} = 88$, $N_2 = \frac{440}{8} = 55$, $N_3 = \frac{440}{11} = 40$.

$88 \equiv 3 \bmod 5$, and $c_1 \equiv 2 \bmod 5$ is the inverse of $3 \bmod 5$.

$55 \equiv 7 \bmod 8$ and $c_2 \equiv 7 \bmod 8$ is the inverse of $7 \bmod 8$.

$40 \equiv 7 \bmod 11$ and $c_3 \equiv 8 \bmod 11$ is the inverse of $7 \bmod 11$.

Then $x = 3 \cdot 88 \cdot 2 + 2 \cdot 55 \cdot 7 + 9 \cdot 40 \cdot 8 = 4178 \equiv 218 \bmod 440$.

2. Find the primitive roots of 1 mod 19.

Solution. When writing this problem, I did not realize that on a calculator, many of the numbers required calculations get converted to exponential notation, which makes them difficult to calculate mod 19. Therefore, any effort at all on this problem will yield full value. The answer to this problem is 3, 15, 2, 10, 14, 13, as these are the numbers whose order mod 19 is 18.

We did not prove this, but if a is a primitive root of one mod p, then so is a^r, for any r relatively prime to $p-1$, and this accounts for all such primitive roots. Thus, in the present case, it is easily seen that 3 is a primitive root mod 19, therefore, $3, 3^5, 3^7, 3^{11}, 3^{13}, 3^{17}$ are the primitive roots of 1 mod 19, which, mod 19, are the numbers above.

3. Determine whether or not the polynomial $f(x) = 3x^2 + 4x - 10$ has a root modulo 137.

Solution. We first look at the discriminant of $f(x)$, i.e., $4^2 - 4 \cdot 3 \cdot (-10) = 136$. To determine if 136 is a square mod 137, we calculate: $(\frac{136}{137}) = (\frac{2}{137})(\frac{2}{137})(\frac{2}{137})(\frac{17}{137}) = 1 \cdot 1 \cdot 1 \cdot (\frac{17}{137})$. And: $(\frac{17}{137}) = (-1)^{8 \cdot 68}(\frac{137}{17}) = (\frac{1}{17}) = 1$. Thus, 136 is a square mod 137. Moreover, since GCD $(2 \cdot 3,\, 137) = 1$, 2 has an inverse mod 137. Thus, we can use the quadratic formula mod 137 to see that $f(x)$ has a root mod 137.

4. Use Gauss's lemma to calculate $(\frac{12}{13})$. Verify your answer using various properties of the Legendre symbol.

Solution. For Gauss's lemma, we take $\frac{13-1}{2} = 6$, so we consider the set $\{1 \cdot 12, 2 \cdot 12, 3 \cdot 12, 4 \cdot 12, 5 \cdot 12, 6 \cdot 12\}$ $= \{12, 24, 36, 48, 60, 72\}$. We reduce these mod 13, and write them so that their residue classes mod 13 are contained in the interval (-6.5, 6.5). This gives $\{-1, -2, -3, -4, -5, -6\}$. There are 6 negative values in this last set, so by Gauss's lemma, $(\frac{12}{13}) = (-1)^6 = 1$.

On the other hand: $(\frac{12}{13}) = (\frac{4}{13})(\frac{3}{13}) = 1\dot{(} - 1)^{1 \cdot 6}(\frac{13}{3}) = (\frac{1}{3}) = 1$.

5. Apply the division algorithm in the Gaussian integers for $u = 2 + 3i$ and $v = 7 + 6i$, dividing v by u.

Solution. We start by calculating $\frac{v}{u}$ as a complex number. $\frac{7+6i}{2+3i} = \frac{32}{13} - \frac{9}{13}i$. Since $[\frac{32}{13}] = 2$ and $[-\frac{9}{13}] = -1$, we take $q = 2 - i$. Then $7 + 6i = (2 + 3i)(2 - i) + 2i$. Note $N(2i) = 4 < N(2 - i) = 5$.

6. Factor $2 + 6i$ as a unit times a product of Gaussian primes.

Solution. We have

$$\begin{aligned}
2+6i &= 2(1+3i)\\
&= (1-i)(1+i)(1+3i)\\
&= (1-i)(1+i)\{(1+i)+2i\}\\
&= (1-i)(1+i)\{(1+i)+(1+i)(1+i)\}\\
&= (1-i)(1+i)\{(1+i)(2+i)\}\\
&= (1-i)(1+i)^2(2+i)
\end{aligned}$$

Note that $1-i, 1+i, 2+i$ are Gaussian primes since their norms are prime integers.

Proof problem. State and prove Euler's Quadratic Residue Theorem. (25 points)

Solution. Euler's QRT states that if p is an odd prime and $\mathrm{GCD}(a,p)=1$, then a is a quadratic residue mod p if and only if $a^{\frac{p-1}{2}} \equiv 1 \bmod p$. For a proof, note that if a is a quadratic residue mod p, say $a \equiv b^2 \bmod p$, then $a^{\frac{p-1}{2}} \equiv (b^2)^{\frac{p-1}{2}} \equiv b^{p-1} \equiv 1 \bmod p$, by the first Fermat's theorem.

Now suppose $a^{\frac{p-1}{2}} \equiv 1 \bmod p$. Take $1 < b \leq p-1$ a primitive root of 1, so that $p-1$ is the order of b mod p. We saw in class that $b^2, b^4, \ldots, b^{p-1}$ are the quadratic residues mod p. Suppose a is not a quadratic residue mod p. Then $a \equiv b^{2k+1} \bmod p$, for some k. Thus, $a^{\frac{p-1}{2}} \equiv b^{\frac{p-1}{2}\cdot 2k+1} \equiv b^{(p-1)k} b^{\frac{p-1}{2}} \equiv b^{\frac{p-1}{2}} \bmod p$, thus $b^{\frac{p-1}{2}} \equiv 1 \bmod p$, contradicting the primitive root property of b.

Alternately: Since b is a primitive root of 1 mod p, $a \equiv b^r \bmod p$, for some r. We want r to be even. We have $1 \equiv a^{\frac{p-1}{2}} \equiv b^{\frac{r(p-1)}{2}}$, so $p-1$ divides $\frac{r(p-1)}{2}$, since $p-1$ is the order of b mod p. Thus $(p-1)d = \frac{r(p-1)}{2}$, for some d, which gives $r = 2d$, and even number, as required.