Mathematics 411

9 December 2005

Final exam preview

Instructions: As always in this course, clarity of exposition is as important as correctness of mathematics.

1. Recall that a *Gaussian integer* is a complex number of the form $a+bi$ where a and b are integers. The Gaussian integers form a ring $\mathbf{Z}[i]$, in which the number 3 has the following special property:

   > Given any two Gaussian integers r and s, if 3 divides the product rs, then 3 divides either r or s (or both).

   Use this fact to prove the following theorem:

   > For any integer $n \geq 1$, given n Gaussian integers r_1, r_2, $\ldots$, r_n, if 3 divides the product $r_1 \cdots r_n$, then 3 divides at least one of the factors r_i.

2. (a) Use the Euclidean algorithm to find an integer solution to the equation

   $$7x + 37y = 1.$$

   (b) Explain how to use the solution of part (a) to find a solution to the congruence

   $$7x \equiv 1 \pmod{37}.$$

   (c) Use part (b) to explain why $[7]$ is a unit in the ring $\mathbf{Z}_{37}$.

3. Given a Gaussian integer t that is neither zero nor a unit in $\mathbf{Z}[i]$, a factorization $t = rs$ in $\mathbf{Z}[i]$ is *nontrivial* if neither r nor s is a unit.

   (a) List the units in $\mathbf{Z}[i]$, indicating for each one what its multiplicative inverse is. No proof is necessary.

   (b) Provide a nontrivial factorization of 53 in $\mathbf{Z}[i]$. Explain why your factorization is nontrivial.

   (c) Suppose that p is a prime number in $\mathbf{Z}$ that has no nontrivial factorizations in $\mathbf{Z}[i]$. Prove that the equation

   $$x^2 + y^2 = p$$

   has no integer solutions. (For full credit, do this from scratch: you shouldn't need to cite any results from the book.)

4. Suppose that R is a ring with additive identity 0. An element r of R is called a *zero-divisor* if r is nonzero and if there is a nonzero element s of R such that $rs = 0$.
   (a) Find a zero-divisor in $\mathbf{Z}_{10}$ and explain why it is one.
   (b) Suppose that $m \geq 2$ is an integer that is not a prime. Describe a zero-divisor in $\mathbf{Z}_m$ and explain why it is one.
   (c) Suppose that p is a prime number. Recall that if p divides a product ab of two integers, then it divides at least one of a and b. Use this to prove that there are no zero-divisors in $\mathbf{Z}_p$.

5. One can construct a ring R with six elements: $R = \{a, b, c, d, e, f\}$, with multiplication table as follows:

$\times$	a	b	c	d	e	f
a	a	a	a	a	a	a
b	a	b	c	a	b	c
c	a	c	b	a	c	b
d	a	a	a	d	d	d
e	a	b	c	d	e	f
f	a	c	b	d	f	e

   (a) Which element of R is the multiplicative identity? Why?
   (b) Which elements of R are units? Why?
   (c) Is R a field? Why or why not?
   (d) Can the multiplication table above be the multiplication table of $\mathbf{Z}_6$, with the six elements of $\mathbf{Z}_6$ being assigned (somehow) the names a, b, c, d, e, and f?

6. In this problem, ϕ represents the Euler phi-function and m is a positive integer.
   (a) Define $\phi(m)$.
   (b) Suppose $m = p^e$ for some prime number p and positive integer e. State a formula for $\phi(m)$ in terms of p and e, and prove that the formula is correct. (For full credit, do this from scratch: you shouldn't need to cite any results from the book.)
   (c) State Euler's theorem. Make sure that all of the terms occurring are clearly identified and any restrictions on them are described.
   (d) Use Euler's theorem to find the smallest positive integer c such that

$$5^{773} \equiv c \pmod{121}.$$

   Explain what you are doing in your calculation, pointing out in particular how Euler's theorem is used.