Mathematics 243, section 1 – Algebraic Structures
Information on Exam 2
October 29, 2003

General Information

The second exam this semester will be given next Wednesday, November 5. The exam will cover the material we have discussed since the first exam, through class on Monday, October 27. This is basically all the material in Chapter 2. Note: This exam may also contain a problem on the technique of proof by mathematical induction. The topics to review are:

1) Properties of $\mathbf{Z}$
2) Proof by mathematical induction
3) Divisibility. Know the statement of the Division Algorithm (Theorem 2.10 in the text) and its proof,
4) Prime numbers, prime factorizations and the "Fundamental Theorem of Arithmetic" (Theorem 2.18),
5) Greatest common divisors and Euclid's algorithm for $\gcd(a, b)$
6) Congruence mod n and the integers mod n ($\mathbf{Z}_n$)
7) Applications to cryptography (affine and RSA encryption and decryption)

Some Review Problems

From Gilbert and Gilbert:

1) Section 2.1: 19, 20
4) Section 2.2: 3, 4, 21, 23
5) Section 2.3: problems like 1-11, proofs like 16,17,18, 20, 27, 32
6) Section 2.4: problems like 2,3, 9, 13
7) Section 2.5: problems 3-18, 27, 29
8) Section 2.6: problems like 3,4,5,6,7
9) Section 2.8: be prepared to encrypt or decrypt one or two symbols using an affine or RSA system. Know how to find the decryption function if the encryption function is given, etc.

Review Session

I will be happy to run a review session before the exam. Our regular problem session time on Monday evening is probably the best time for this.

I.

A) Given integers a, and $b > 0$, prove that there exist unique integers q and r such that $a = qb + r$ and $0 \leq r < b$. (You may apply the Well-Ordering Principle without justifying that.)

B) Find the quotient q and the remainder r as in part A for $a = 4578$ and $b = 235$.

II.

A) Give the definition of the *greatest common divisor* of the integers a, b.

B) Find the integer $d = \gcd(488, 376)$ and express d in the form $d = m \cdot 488 + n \cdot 76$ for integers m, n.

C) Prove that if there is a solution of the congruence $ax \equiv b \pmod{n}$ (where $n > 1$), then $\gcd(a, n) | b$.

III. Find all solutions $[x]$ of the equation $[17][x] + [4] = [5]$ in $\mathbf{Z}_{29}$.

IV. In an RSA public key cryptosystem, the public key information is $m = 143$ and $e = 19$. Messages consisting of capital roman letters and blanks are encoded as 3-digit blocks $000, 001, \cdots, 026$ and encrypted as 3-digit blocks.

A) How would the letter G be encrypted?

B) If a block 102 is received, what letter does that decrypt to?

Extra Credit

Show that an integer n is congruent to 0 mod 3 if and only if the sum of its base 10 digits is congruent to 0 mod 3. (For instance, 6843 has digit sum $6 + 8 + 4 + 3 = 21 \equiv 0 \pmod{3}$, and $6843 = 3 \cdot 2281$.)