MATH 311W

Hints and Partial Solutions to Some Homework Problems

Gary L. Mullen

Fall Semester 2006

1.1.1 Part (iii); the other parts are done the same way. $126 = 1(91) + 35$

$91 = 2(35) + 21$

$35 = 1(21) + 14$

$21 = 1(14) + 7$

$14 = 2(7) + 0$

Thus $(91, 126) = 7$, the last nonzero remainder.

Now to write the gcd $(91, 126) = 7$ as a combination of 91 and 126, one works backwards starting with the next to last line of the above calculation. We have

$7 = 21 - 1(14) = 21 - 1(35 - 1(21) = 2(21) - 1(35) = 2(91 - 2(35) - 1(35) = 2(91) - 5(35) = 2(91) - 5(126 - 1(91) = 7(91) - 5(126)$. Notice as a check that $7(91) - 5(126) = 637 - 630 = 7$.

1.1.2 $(6, 14) = 2$ and $(2, 21) = 1$ so $(6, 14, 21) = 1$

1.1.3 If $(a, b) = 1$ and k is an integer, show that $(b, a + bk) = 1$. Assume $(b, a + bk) = d$ so d divides b. Then d divides $a + bk$ so that we will also have d dividing $a + bk - bk = a$, but this means that $d = 1$ since now $d|a$ and $d|b$.

1.1.4 Show that if $a|bc$ then it is not necessarily true that $a|b$ or $a|c$. For example $8|(4)(2)$ but $8 \not| 4$ and $8 \not| 2$

1.1.5 Show that if $a|c$ and $b|c$ then it is not necessarily true that $ab|c$. For example, $2|4$ and $4|4$, but $2(4) = 8 \not| 4$.

1.1.6 If $(a, c) = 1 = (b, c)$, show that $(ab, c) = 1$. Assume an integer d divides ab and d divides c. Since $(b, c) = 1$ it implies that $d|a$ and hence $d = 1$.

1.1.7 We have two water jugs, one holds 12 units and the other 17 units. Start

with both empty which we represent as 0 0, then fill the larger to get 0 17, then continuing 12 5, 0 5, 5 0, 5 17, 12 10, 0 10, 10 0, 10 17, 12 15, 0 15, 12 3, 0 3, 3 0, 3 17, 12 8, 0 8 and we are done. Notice that this really says $8 = 4(17) - 5(12)$ so it is a gcd kind of problem.

1.2.1 $a_1 = 1$ and $a_{n+1} = 2a_n + 1$ for $n \geq 1$. Notice that the text says $n \geq 2$ but then we would have $a_3 = 2a_2 + 1$ but no way to tie this into the value of a_1.

The first few values give $a_1 = 1, a_2 = 3, a_3 = 7, a_4 = 15, a_5 = 31, \ldots$. Use induction to show that $a_n + 1$ is always a power of 2, i.e a number of the form 2^e for some $e \geq 0$.

First for $n = 1$, we have $1 + 1 = 2 = 2^1$ fine.

Assume that $a_k + 1 = 2^b$ for some b. Then we have

$$a_{k+1} + 1 = 2a_k + 1 + 1 = 2(2^b - 1) + 1 + 1 = 2^{b+1} - 2 + 1 + 1 = 2^{b+1}$$

and we are done.

1.2.2 This was done in class but here it is again. Show that $1 + 4 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}$

First note that $1 = \frac{1(2)(3)}{6}$

Assume true for k so we would have

$$1 + 4 + \cdots + k^2 = \frac{k(k+1)(2k+1)}{6}$$

Then we have

$$1 + 4 + \cdots + k^2 + (k+1)^2 = \frac{k(k+1)(2k+1)}{6} + (k+1)^2,$$

which after some simplification, gives $\frac{(k+1)(k+2)(2k+3)}{6}$ and we are done.

1.2.3 $f_1 = 1, f_2 = 1, f_{n+2} = f_{n+1} + f_n, n \geq 1$

For $n = 1$ clearly $(f_1, f_2) = (1, 1) = 1$

Assume $(f_k, f_{k-1}) = 1$. Show $(f_{k+1}, f_k) = d = 1$. Note that if d divides f_{k+1} and f_k then since $f_{k+1} = f_k + f_{k-1}$, then d divides f_k and f_{k-1}, a contradiction of the induction hypotheses.

1.2.3 The Fibonacci numbers are defined by $f_k = f_{k-1} + f_{k-2}$, i.e the next is the sum of the previous two. Now use induction.

1.2.4 This is a good problem to illustrate how one can sometimes find the statement $P(n)$ so that one can then apply induction. This problem involves a lot of algebra, but the idea is easy. Assume

$$1^3 + 2^3 + \cdots + n^3 = an^4 + bn^3 + cn^2 + dn + e,$$

for some a, b, c, d, e. Then

$$1^3 + 2^3 + \cdots + n^3 + (n+1)^3 = an^4 + bn^3 + cn^2 + dn + e + (n+1)^3$$

$$= an^4 + (b+1)n^3 + (c+3)n^2 + (d+3)n + (e+1).$$

This must also equal $a(n+1)^4 + b(n+1)^3 + c(n+1)^2 + d(n+1) + e$.

Now expand this out and collect like powers of n and equate coefficients to obtain $b+1 = 4a+b$ so that $a = 1/4$. Similarly $c+3 = 6a+3b+c$ so that after simplification, $3 = 6b$ so $b = 1/2$. Similarly we will obtain $c = 1/4$ and $d = e = 0$.Thus

$$1^3 + 2^3 + \cdots + n^3 = \frac{n^4}{4} + \frac{n^3}{2} + \frac{n^2}{4} = [\frac{n(n+1)}{2}]^2$$

.

1.2.5 Use math. induction to show that

$$\frac{1}{3}+\frac{1}{15}+\cdots+\frac{1}{(2n-1)(2n+1)}=\frac{n}{2n+1}.$$

For $n=1$ we have $\frac{1}{1(3)}=\frac{1}{1(3)}$. Assume true for $n=k$ and then for $n=k+1$ we have

$$\frac{1}{3}+\cdots+\frac{1}{(2k-1)(2k+1)}+\frac{1}{(2k+1)(2k+3)}.$$

Now by the induction hypotheses this becomes equal to

$$\frac{k}{2k+1}+\frac{1}{(2k+1)(2k+3)}$$

which after simplification becomes $\frac{k+1}{2(k+1)+1}$, and we are done.

1.2.6 Find formula for $1+3+\cdots+2n-1$, the sum of the first n odd positive integers. Here is a proof without induction. This sum will equal the expression

$$1+2+\cdots+2n-1-(2+4+\cdots+2n-2),$$

i.e. the sum of all the numbers $\leq 2n-1$ minus the sum of the even ones up to that point. Now simplify this expression to obtain n^2.

Here is another proof by induction, but notice here that we have to have, or guess, the formula to try and prove it by induction. Ok, we speculate from the above that $1+3+\cdots+2n-1=n^2$. This is clearly true for $n=1$, and so assume it is true for $n=k$ so that we have $1+3+\cdots+2k-1=k^2$. Then for $n=k+1$ we have $1+3+\cdots+(2k-1)+(2k+1)=k^2+2k+1=(k+1)^2$ and we are done.

1.2.7 Show that if $x\neq 1$,

$$1+x+x^2+\cdots+x^n=\frac{1-x^{n+1}}{1-x}=\frac{x^{n+1}-1}{x-1}.$$

By induction, when $n = 1$, $1 + x = (x^2 - 1)/(x - 1)$.

Assume true for k; then for $k + 1$ we have

$$1 + x + x^2 + \cdots + x^k + x^{k+1} = \frac{x^{k+1} - 1}{x - 1} + x^{k+1} = \frac{x^{k+2} - 1}{x - 1}$$

and we are done.

1.2.8 (i) Show $n^5 - n$ is divisible by 5 for any positive integer n. Use induction.

When $n = 1$ we have $1^5 - 1 = 0 = 0(5)$ ok. Assume now for k that $k^5 - k$ is divisble by 5 so it equals say $5M$ for some integer M. Now for $k+1$ we have with some algebra, $(k+1)^5 - (k+1) = k^5 - k + 5k^4 + 10k^3 + 10k^2 + 5k = 5M + 5k^4 + 10k^3 + 10k^2 + 5k = 5(X)$ for some integer X so is divisible by 5.

For part (ii) show $3^{2n} - 1$ is divisible by 8. Use induction which is true when $n = 1$ since $9 - 1 = 8 = 8(1)$. Assume for k that $3^{2k} - 1 = 8M$ for some M. Then

$$3^{2(k+1)} - 1 = 3^{2k+2} - 1 = (3^{2k} - 1)3^2 + 8 = 8M3^2 + 8 = 8(9M + 1).$$

1.2.9 Let $x_0 = 2, x_1 = 5$ and in general $x_{n+2} = 5x_{n+1} - 3x_n, n \geq 0$. This is called a *linear recurrence of order two*. Show that $2^n x_n = (5 + \sqrt{13})^n + (5 - \sqrt{13})^n$. Use strong induction. Check this is true for $n = 0, 1$. For $n = 0; 2 = 1 + 1$. For $n = 1, 2x_1 = 10 = (5 + \sqrt{13}) + (5 - \sqrt{13})$. Assume true for $m \leq k$ so that we have $2^m x_m = (5 + \sqrt{13})^m + (5 - \sqrt{13})^m$ for each value of $m \leq k$. For $k + 1$ we have

$2^{k+1} x_{k+1} = 2^{k+1}(5x_k - 3x_{k-1})$ (Here I used $n = k - 1$ in the recursion), which becomes $= (10)2^k x_k - (12)2^{k-1} x_{k-1}$. Now use the induction step with $m = k$ and $m = k - 1$. After a bunch of algebra and simplification becomes $(5 + \sqrt{13})^{k+1} + (5 - \sqrt{13})^{k+1}$ and we are done.

1.2.11 False when $n = 11$ since $2^{11} - 1 = 23(89)$.

1.3.1 I'm too lazy to do this up to 250, see the list in the back of our text!!!

1.3.2 If $n = ab$ then both a and b can't be less than $\sqrt{n}$ or else $ab < n$.

1.3.3 Let's work on the pair 136 and 150; the others are similar. Ok first $136 = 2^3(17)$ and $150 = 2(3)(5^2)$. Thus $gcd(136, 150) = (136, 150) = 2$ and $lcm[136, 150] = [136, 150] = 2^3(3)(17)(5^2$. Note that the gcd is obtained by taking each prime to the minimum power it occurs in the two numbers, and the lcm is obtained by taking each prime to the maximum it occurs in each number.

Also note that $(136, 150)[136, 150] = 136(150)$ so if one has one of the gcd or the lcm, one can quickly get the other.

1.3.4 If $p_1 = 2, p_2 = 3, \ldots$ is the list of primes, show that $c_n = p_1 \times \cdots \times p_n + 1$ is a prime for $n = 1, \ldots, 5$ but not for $n = 6$. You check that it works for the first five values, for example $c_1 = 3, c_2 = 7$ etc., but $c_6 = 30031 = 59(509)$ is not a prime.

1.3.5 If $(n, a) = 1$ and $(n, b) = 1$, show that $(n, ab) = 1$. Assume p is a prime which divides both n and ab. Hence p must divide a or p must divide b. Hence either

Case 1: $p|n$ and $p|a$ so that $(n, a) > 1$ or

Case 2: $p|n$ and $p|b$ so that $(n, b) > 1$, and both are contradictions.

1.3.6 If $2^n - 1$ is a prime, show that n is a prime. Suppose that n is not a prime so that $n = ab$, with $1 < a, b < n$. Then

$$2^n - 1 = 2^{ab} - 1 = (2^a - 1)(2^{a(b-1)} + 2^{a(b-2)} + \cdots + 2^a + 1),$$

which is a contradiction if $2^n - 1$ is a prime.

1.3.7 If $2^n + 1$ is a prime for some $n \geq 1$, show that $n = 2^k$ for some k, i.e. n must be a power of 2. Assume that $n = 2^k a$ with $a \geq 1$ being odd.

Convince yourself that we can factor $x^a + 1$ as follows.

$$x^a + 1 = (x + 1)(x^{a-1} - x^{a-2} + \cdots - x + 1)$$

The signs alternate in the big expression on the right.

You can of course check that this factorization is correct by multiplying it out, but how did I find it? Just use long division and divide x^a+1 by $x+1$ and see what happens.

Now let $x = 2^{2^k}$ so we have

$$(2^{2^k})^a + 1 = 2^{2^k a} + 1 = (2^{2^k} + 1)(2^{2^k(a-1)} - 2^{2^k(a-2)} + \cdots - 2^{2^k} + 1).$$

If $a > 1$, the RHS consists of two terms, each > 1 so the LHS is not a prime.

But if $a = 1$ the RHS can indeed be a prime.

1.3.8 We model our proof after Euclid's proof that there are infinitely many primes. Assume there are only finitely many primes of the form $4k+3$ and suppose that $p_1, \ldots, p_n$ are all of them. Form the number $N = 4p_2 \ldots p_n + 3$. If N is a prime we are done. If N is not a prime, it has a unique factorization into a product of primes. If all of the primes dividing N were of the form $4m+1$, then N would also be of the form $4M+1$, which it isn't. Hence there must be at least one prime p of the form $4m+3$ which divides N. But then $p = p_i$ for some i, and thus p must divide 3, a contradiction.

Why doesn't this kind of argument work to show that there are infinitely many primes of the form $4k+1$?

1.3.9 Show that $(a,b)[a,b] = ab$. First factor $a = p_1^{e_1} \ldots p_r^{e_r}$ and $b = p_1^{f_1} \ldots p_r^{f_r}$. Convince yourself why we can assume that a and b both have the same primes $p_1, \ldots, p_r$.

Also convince yourself that the $min\{a,b\} + max\{a,b\} = a + b$. Then

$$ab = p_1^{e_1+f_1} \ldots p_r^{e_r+f_r} = p_1^{min\{e_1,f_1\}+max\{e_1,f_1\}} \ldots p_r^{min\{e_r,f_r\}+max\{e_r,f_r\}}$$

and we are done.

1.4.1 Remember that to check if $a \equiv b \pmod{n}$, one calculates $a - b$ and checks whether this is divisible by n. For example for part (ii), is $-8 \equiv 48 \pmod{14}$? Well $-8 - 48 = -56 = 14(-4)$ so yes.

1.4.2 See text

1.4.3 Do the following have inverses? For example, in part (ii), $(10, 26) = 2 > 1$ so no inverse. For part (iii) $(11, 31) = 1$ so it is easy to determine that 11 has an inverse mod 31, but how to find it? This method will always work to get inverses.

$31 = 2(11) + 9$

$11 = 1(9) + 2$

$9 = 4(2) + 1$

so $(11, 31) = 1$ and thus 11 has an inverse mod 31. Now work backwards to locate the inverse of 11. We have

$1 = 9 - 4(2) = 9 - 4(11 - 1(9)) = 5(9) - 4(11) = 5(31 - 2(11)) - 4(11) = 5(31) - 14(11)$. Thus the inverse of 11 mod 31 is -14, but we want the inverse to lie between 1 and 30 so we convert -14 to 17 since $-14 \equiv 17 \pmod{31}$. Thus the inverse of 11 is 17 mod 31.

1.4.4 For $n = 16$, $G_{16} = Z_{16}^* = \{1, 3, 5, 7, 9, 11, 13, 15\}$, the set of all elements < 16 which are relatively prime to 16, and so now write out the 8×8 multiplication table modulo 16.

For $n = 15$, $G_{15} = Z_{15}^* = \{1, 2, 4, 7, 8, 11, 13, 14\}$ and now write out the 8×8 multiplication table modulo 15.

1.4.5 Show that a number of the form $8n + 7$ cannot be the sum of three squares. Assume that $8n + 7 = a^2 + b^2 + c^2$. Now consider the last digit of the number which must be one of the values ; $0, 1, 2, 3, 4, 5, 6, 7, 8, 9$. Now square each of these last digits and reduce mod 8 to obtain in order, $0, 1, 4, 1, 0, 1, 4, 1, 0, 1$.

Now notice that no sum of three of these add up to 7 modulo 8, and we are done.

1.4.6 Show that $x^2 \equiv 1 \pmod{p}$ has exactly two solutions if p is a prime. We

have $p|(x^2-1) = (x+1)(x-1)$. But since p is a prime, p must divide one factor or the other, thus $x = 1$ or $x = -1$.

Find an example to show that this result is not true if p is not a prime.

1.4.7 Show that if p is a prime, then $(p-1)! \equiv -1 \pmod{p}$. Notice that

$$(p-1)! = 1(2)(3)\dots(p-3)(p-2)(p-1)$$

Each element a with $1 \leq a \leq p-1$ has a unique inverse a^{-1} so that $aa^{-1} \equiv 1 \pmod{p}$, and unless $a = 1$ or $a = -1 = p-1$, $a \neq a^{-1}$. And from the above problem if $a = a^{-1}$, then $a^2 = 1$ and so $a = 1$ or $a = -1$. Thus $(p-1)! \equiv 1(p-1) \equiv -1 \pmod{p}$ and we are done.

1.4.9 Casting out nines. Why it works?If $n = a_k(10)^k + a_{k-1}(10)^{k-1} + \cdots + a_1 10 + a_0$, then $n \equiv a_k + \cdots + a_0 \pmod{9}$, since each of the powers of 10 is congruent to 1 mod 9.

1.5.1 (1) $(3, 12) = 3$ and $3 \not| 1$ so no solution.

(ii) Solve $3x \equiv 1 \pmod{11}$. Since $(3, 11) = 1$ and $1|1$, there is one solution mod 11 which is $x = 4$.

(iii) Solve $64x \equiv 32 \pmod{84}$. Since $(64, 84) = 4$ and $4|32$, there are four solutions mod 84 which can be obtained as follows. First divide by 4 to obtain $16x \equiv 8 \pmod{21}$. Here $x = 11$ is a solution mod 21, which can be found using the fact that $(16, 21) = 1$. Hence $n/d = 84/4 = 21$ so the four distinct solutions mod 84 are given by $x = 11, 32, 53, 74$ mod 84.

(iv) Solve $15x \equiv 5 \pmod{17}$. Since $(15, 17) = 1$, there is one solution mod 17. The usual calculation shows that $15^{-1} \equiv 8 \pmod{17}$ so that $x = 5(8) \equiv 40 \equiv 6 \pmod{17}$.

(v) Solve $15x \equiv 5 \pmod{18}$. Since $(15, 18) = 3 \not| 5$, there is no solution.

(vi) Solve $15x \equiv 5 \pmod{100}$. Since $(15, 100) = 5|5$, there will be five solutions

mod 100. And $n/d = 100/5 = 20$. Dividing the original congruence by 5 yields $3x \equiv 1 \pmod{20}$ which has $x = 7$ as a solution mod 20. Hence the five distinct solutions mod 100 are given by $x = 7, 27, 47, 67, 87 \pmod{100}$.

(vii) Solve $23x \equiv 16 \pmod{107}$ $(23, 107) = 1$ so one solution. First get the inverse of 23 mod 107, which is 14. Then $x = 14(16) \equiv 224 \equiv 10 \pmod{107}$.

1.5.2 (i) Solve

$$x \equiv 4 \pmod{24}$$

$$x \equiv 7 \pmod{11}$$

So $x = 4 + 24k \equiv 7 \pmod{11}$. This yields $2k \equiv 3 \pmod{11}$ so $k \equiv 7 \pmod{11}$ and thus $x \equiv 4 + 24(7) \equiv 172 \pmod{264}$.

(ii) Solve

$$3x \equiv 1 \mod 5$$

$$2x \equiv 6 \pmod{8}$$

I would first divide the second congruence by two and work with $x \equiv 3 \pmod{4}$, which leads to $x = 3 + 4k$. Substitute this into the first congruence to obtain $9 + 12k \equiv 1 \pmod{5}$, which leads to $k = 1$ and hence $x \equiv 7 \pmod{20}$.

1.5.2 (iii) To solve this system of three simultaneous congruences, start with $x = 3 + 5k$ from the first, and plug this into the third to obtain $k \equiv 0 \pmod{8}$ so that $x = 3 + 40M$ for the solution to the first and third congruences. Now plug this into the second which will yield $2(3 + 40M) \equiv 1 \pmod{7}$ which yields $M = 3$ and so finally $x = 3 + 40(3) = 123 \pmod{280}$.

1.5.3 You need to simultaneously solve the following congruences $x \equiv 8 \pmod{11}; x \equiv 4 \pmod{10}; x \equiv 0 \pmod{2}7$, whose solution will be 1944, mod 2970.

1.5.4 (i) Show $x^4 + x^2 + 1$ has no integer roots. This expression is > 0 for any x.

Remember that a is a root of a polynomial iff $x-a$ is a factor. Hence 1 and 2 are roots (actually multiple roots) mod 3, so it factors as $(x-1)^2(x-2)^2 = (x+1)^2(x+2)^2$ when factored modulo 3.

(ii) Show $f(x) = 7x^3 - 6x^2 + 2x - 1 = 0$ has no integer solution. Calculate modulo 3 to obtain $f(0) = -1, f(1) = 2, f(2) \equiv 2$ so no solution mod 3, and thus no integer solution.

1.5.5 Solve the system $x \equiv 3 \pmod{15}; x \equiv 2 \pmod{7}, x \equiv 0 \pmod{4}$ to obtain 408.

Section 1.6

Remember that the order of an element a mod n is the smallest positive integer t so that $a^t \equiv 1 \pmod{n}$. And also recall that an element a will have finite order mod n iff $(a, n) = 1$. Unfortunately there is no known easy method for finding the order of elements. Ok, now for some problems.

1.6.1 (1) 2 mod 31. Just calculate powers of 2 mod 31 and you will soon find that $2^5 \equiv 1 \pmod{31}$ so the order is 5.

(ii) 10 mod 91. $(10)^2 \equiv 9 \pmod{91}$ so $(10)^3 \equiv 90 \equiv -1 \pmod{91}$. Hence $(10)^6 \equiv 1 \pmod{91}$ so the order is 6.

(iii) 7 mod 51. Note that $\phi(51) = \phi(3)\phi(17) = 2(16) = 32$. Since the order must now divide 32, it must be a power of 2, and one checks that $7^2 = -2$ so $7^4 = 4, 7^8 = 16$, and then $7^{16} \equiv 1 \pmod{51}$ so the order is 16.

(iv) 2 mod 41. Note that 41 is a prime. Hence $2^{40} \equiv 1 \pmod{41}$ and hence the order must divide 40. Now do some calculations to show that the $2^{20} \equiv 1 \pmod{41}$ and this is the smallest exponent giving 1 so the order is 20.

1.6.2 Calculate (i) 5^{20} mod 7. We know that $5^6 \equiv 1 \pmod{7}$ so $5^{20} \equiv 5^2 \equiv 4 \pmod{7}$.

(ii) $2^{16} \pmod{8}$. Note that $2^{16} = 2^3(2^{13}) \equiv 0 \pmod{8}$

(iii) $7^{1001} \pmod{11}$ Note that $7^{10} \equiv 1 \pmod{11}$ so $7^{1001} \equiv (7^{10^3})7 \equiv 7 \pmod{11}$.

(iv) $6^{76} \pmod{13}$. Note that $6^{12} \equiv 1 \pmod{13}$ so $6^{76} \equiv 6^4 \equiv 10(10) \equiv (-3)(-3) \equiv 9 \pmod{13}$.

1.6.3 Show that a^5 and a have the same last digit. Thus we must show that they are congruent modulo 10. Let $a = 10k + d$ so the last digit is d. Note that $a^5 \equiv (10k+d)^5 \equiv d^5 \pmod{10}$. Also note that $d^5 \equiv d \pmod{2}$ and $d^5 \equiv d \pmod{5}$ so $d^5 \equiv d \pmod{10}$. Here I have used the fact that if $(a, b) = 1$ and $a|n$ and $b|n$, then $(ab)|n$.

1.6.4 By the binomial Theorem expand $(x + y)^p$ and then show that if p is a prime, all of the terms except the first and the last are congruent to 0 mod p and hence if one replaces both x and y by 1, we obtain $2^p \equiv (1+1)^p \equiv 1^p+1^p \equiv 1+1 \equiv 2 \pmod{p}$.

1.6.5. $\phi(32) = \phi(2^5) = 2^5 - 2^4 = 16$.

$\phi(21) = \phi(3)\phi(7) = 2(6) = 12$.

$\phi(120) = \phi(3(5)(2^3)) = \phi(3)\phi(5)\phi(2^3) = 2(4)(8-4) = 2(4)(4) = 32$

$\phi(384) = \phi(2^7(3)) = \phi(2^7)\phi(3) = (2^7 - 2^6)(2) = 64(2) = 128$.

1.6.6 (i) Find $2^{25} \pmod{21}$. Note that $\phi(21) = 12$ so $2^{12} \equiv 1 \pmod{21}$. Hence $2^{25} \equiv 2^{12}2^{12}2 \equiv 2 \pmod{21}$.

(ii) Find $7^{66} \pmod{120}$ $\phi(120) = \phi((3(5)(8)) = 2(4)(4) = 32$. Then $7^{66} \equiv 7^{64}7^2 \equiv 49 \pmod{120}$.

(iii) Find the last two digits of $1 + 7^{162} + 5^{121} \times 3^{312}$. We work mod 100 and check first that $\phi(100) = 40$. Hence $1 + 7^{162} \equiv 1 + 49 \equiv 50 \pmod{100}$. Now notice that if $k \geq 2$, then $5^k \equiv 25 \pmod{100}$. Also $25 \times 81 \equiv 25 \pmod{100}$. Thus the part involving the huge powers on 5 and on 3 just reduces to 25 mod 100. Hence the entire mess reduces to $50 + 25 \equiv 75 \pmod{100}$ and we are done.

1.6.7 Show that for every positive integer n that $n^{13} - n$ is divisible by 2,3,5,7,13. For $n = 13$, this follows immediately from Fermat's Theorem. I'll provide a solution for say $n = 5$, the other values of n can be handled in similar ways. Since 5 is a

prime, we know that $n^4 \equiv 1 \pmod 5$ and hence $n^{13} \equiv (n^4)^3 n \equiv n \pmod n$.

1.6.8 If $n \geq 2$ show that if p is a prime which divides n but is such that p^2 does not divide n, then $p^{\phi(n)+1} \equiv p \pmod n$. Write $n = pm$ with $(p, m) = 1$. From Euler's Theorem we have $p^{\phi(m)} \equiv 1 \pmod m$, so that $p^{\phi(m)} - 1 = mK$ for some K. Hence $p^{(p-1)\phi(m)} - 1 = mM$ for some M, and thus $p^{\phi(n)} - 1 = mM$. Hence we have that $p^{\phi(n)+1} - p = mpM$ so that $p^{\phi(n)+1} \equiv p \pmod n$.

For an extension of this result use the same strategy. Let $n = am$ with $(a, m) = 1$ so that $a^{\phi(m)} \equiv 1 \pmod m$. Then $a^{\phi(m)} - 1 = mK$ and so $a^{\phi(a)\phi(m)} - 1 = mM$. Hence we have $a^{\phi(n)+1} - a = amM$ from which it follows that $a^{\phi(n)+1} \equiv a \pmod n$.

Section 2.1

2.1.1: $X = \{x \in Z | x^3 = x\} = \{0, 1, -1\}$

$Y = \{x \in Z | x^2 = x\} = \{0, 1\}$

$Z = \{x \in Z | x^2 \leq 2\} = \{-1, 0, 1\}$

$W = \{0, 1, -1\}$

$V = \{0, 1\}$

Hence $X = W = Z$ and $Y = V$.

2.1.2: There will be 8 subsets of the set $X = \{a, b, c\}$ These are

$$\phi, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}$$

In general for a set X with n elements, the power set $P(X)$ consisting of all subsets of X will contain 2^n elements (each element of $P(X)$ is a subset). We already proved this in class by using math. induction.

2.1.6: $X = \{0, 1\}, Y = \{2, 3\}$. Then $X \times Y = \{(0, 2), (0, 3), (1, 2), (1, 3)\}$

Since there are four elements in the set $X \times Y$, there will be $2^4 = 16$ subsets of $X \times Y$.

2.1.8: Assume $|X| = m$ and $|Y| = n$. Then since the Cartesian product consists

of all ordered pairs with the first element of the pair coming from X (for which there are m choices), and the second element of the ordered pair coming from Y (for which there are n choices), the two are independent so the total number of pairs will be mn.

2.1.9: Let $A = \{1, 2\} = B$. Let $X = \{(1, 1), (2, 2)\}$ so that X is subset of $A \times B$. Now if $X = C \times D$ and C is a subset of A and D is a subset of B, then $C = \{1\}$ or $\{2\}$ and the same for D, but these don't work.

2.2.1: If $X = \{0, 1, 2\}$ and $Y = \{0, 5\}$ there will be a total of $2^3 = 8$ functions $f : X \to Y$ since we can map each of the three elements $0, 1, 2$ to either 0 or 5. You should actually list the 8 functions.

2.2.2: (i) $f : Z \to Z$ defined by $f(x) = x-1$. This is 1-1 because if $f(x_1) = f(x_2)$ then we have $x_1 - 1 = x_2 - 1$ which implies that $x_1 = x_2$. For onto, let $y \in Z$ then consider $f(y+1) = y+1-1 = y$. Thus f is both 1-1 and onto, thus it is a bijection.

(ii) $f : R \to R^+$, the non-negative reals, defined by $f(x) = |x|$. Not 1-1 since $f(1) = f(-1) = 1$ It is onto because given $y \geq 0, f(y) = |y| = y$.

(iii) $f : R \to R$ defined by $f(x) = |x|$. Not 1-1 for same reason as in previous problem. Not onto since you never get any negative values.

(iv) $f : R \times R \to R$ defined by $f(x, y) = x$. Onto since given any real z, $f(z, z) = z$. Not 1-1 since for example $f(1, 2) = f(1, 1) = 1$.

$f : Z \to Z$ defined by $f(x) = 2x$. Not onto since we never get any odd integers as image values. It is 1-1 since if $2x_1 = 2x_2$, then $x_1 = x_2$.

2.2.3: For (a) this is just the graph of $f(x) = x$ and for (b) the graph of $f(x) = 1$.

2.2.4: Let $f : R \to R$ and $g : R \to R$ be defined by $f(x) = x+1$ and $g(x) = x^2-2$. Then

$$f \circ g = x^2 - 2 + 1 = x^2 - 1$$

$$g \circ f = (x+1)^2 - 2 = x^2 + 2x - 1$$

$$f \circ f = x + 1 + 1 = x + 2$$

$$g \circ g = (x^2 - 2)^2 - 2 = x^4 - 4x^2 + 2$$

2.2.5: In these problems it is helpful to think back to your calculus days for examples of functions with this or that property. There is no particular method for these kinds of problems, other than to think about graphs of various functions.

(i) Use $\log x$

(ii) Use $\tan x$

(iii) $f : N \to Z$ defined by $f(x) = k$ if $x = 2k$ is even, and $-k$ if $x = 2k - 1$ is odd.

2.2.6 Describe all bijections on $S = \{0, 1, 2\}$. Since each element must map to a different value in order to be 1-1, there will be three choices for the image of 0, two for the image of 1 and then the image of 2 will be uniquely determined. In the following I list the elements of S in the top row, and then the $3(2)(1) = 6$ bijections in the next six lines. Each of these six lines is viewed as the image of 0,1,2

0 1 2

---

0 1 2

0 2 1

1 0 2

1 2 0

2 0 1

2 1 0

2.2.7 Find inverses of the following functions. Remember the strategy to do this, which is not always easy to do, is to try and solve for x in the equation $f(x) = y$.

(i) $f(x) = (4 - x)/3 = y$ so after some algebra we have $f^{-1}(y) = 4 - 3y$.

(ii) $f(x) = x^3 - 3x^2 + 3x - 1 = (x - 1)^3 = y$. So we obtain $x - 1 = y^{1/3}$; i.e. $x = y^{1/3} + 1$.

2.2.8 I will explain this problem in class; it is an illustration of an important method of proof called the inclusion/exclusion principle.

2.2.10 Let $A \subseteq X$ and define a function $f_A : X \to \{0, 1\}$ by $f_A(x) = 1$ if $x \in A$ and 0 if $x \notin A$.

(a) Show $A = B$ iff $f_A = f_B$. If $A = B$ then clearly F_A and F_B are both 1 or 0 at the same time so they are equal as functions.

Now in the other direction assume that $f_A = f_B$. We need to show that $A = B$.

Let $a \in A$ so $f_A(a) = 1 = f_B(a)$ so $a \in B$ and thus $A \subseteq B$

Let $b \in B$ so $f_B(b) = 1 = f_A(b)$ so $b \in A$ and thus $B \subseteq A$. Hence $A = B$.

(b) Let A be the subset of X that maps onto $1 = \{x \in X | f(x) = 1\} = f^{-1}(1)$ and then $f(x) = f_A(x)$ and we are done.

2.2.11 The best solution here is to use induction on the number of elements in the set X. We have already done this problem in class as an illustration of math. induction.

2.3.1 In these problems there is no shortcut just always check the following. Reflexsive: Check if xRx holds for all x

Symmetric: Assume xRy and check whether yRx holds.

Transitive: Assume xRy and yRz both hold. Then check whether xRz holds.

(a) $X = Z$ and aRb if $a \leq b + 1$.

$a \leq a + 1$ so ref.

not sym. since $1 \leq 5 + 1$ but clearly $5 \not\leq 1 + 1$.

Let $a = 2, b = 1, c = 0$ Then

$2 \leq 1+1$ and $1 \leq 0+1$ but $2 \not\leq 0+1$ so not trans.

(b) aRb if $a+b$ even

$a+a=2a$ is even so ref.

If $a+b$ even then clearly $b+a$ even so symm.

If $a+b=2k$ is even and $b+c=2m$ is even is $a+c$ even? $a+c=2(k+m-b)$ is even thus trans.

(c) $X=P$ and aRb if $(a,b)=1$.

If $a \neq 1$, $(a,a)=a \neq 1$ so not ref.

It is sym. since $(a,b)=(b,a)$

Not trans. since $(2,3)=1$ and $(3,4)=1$ but $(2,4)=2$

(d)$X=Z$ aRb if $a+b$ div. by 3

Not ref. since $2+2=4$ is not div. by 3.

It is sym since if $a+b$ is div. by 3, so is $b+a$.

Not trans. since $2+1$ is div. by 3 and $1+5$ is div. by 3 but $2+5=7$ is not div. by 3.

(e) aRb if $a^2 \leq b^2$.

$a^2 \leq a^2$ so ref.

$1^2 \leq 2^2$ but $2^2 \not\leq 1^2$ so not sym.

$a^2 \leq b^2$ and $b^2 \leq c^2$ so $a^2 \leq c^2$ so trans.

(f) $X=R \times R$ and $(a,b)R(c,d)$ if $a=c$.

$(a,b)R(a,b)$ since $a=a$ so yes ref.

If $(a,b)R(c,d)$ then $a=c$. Hence $(c,d)R(a,b)$ since $c=a$

If $(a,b)R(c,d)$ and $(c,d)R(e,f)$ then $a=c$ and $c=e$ Hence $(a,b)R(e,f)$ since $a=e$ and so R it is trans.

(g) $X=N \times N$ with $(a,b)R(c,d)$ if $a<c$ or $(a=c$ and $b \leq d)$.

$(a,b)R(a,b)$ since $a=a$ and $b \leq b$ so ref.

For example, $(1,2)R(1,3)$ since $1 = 1$ and $2 \leq 3$ but note that $(1,3)R(1,2)$ does not hold since $3 \not\leq 2$ so not. sym.

Assume $(a,b)R((c,d)$ and $(c,d)R(e,f)$. Then we have

$a < c$ or $(a = c$ and $b \leq d)$

and $c < e$ or $(c = e$ and $d \leq f)$

By checking various cases convince yourself that these imply that

$a < e$ or $(a = e$ and $b \leq f)$ so $(a,b)R(e,f)$ and R is trans.

2.3.3 In the symmetric part where xRy implies yRx, for some value of x, there may not be such an element y.

Section 4.1 As I indicated in my earlier email, these problems all involve simple permutation calculations with cycles and the two rowed notation, and since nothing else is involved, I will not relist the answers here as they are already given in the back of our text.

Section 4.2

4.2.1 (i) disjoint cycles so the order is $\text{lcm}[5,3,2] = 30$, and the sign is

$$((-1)^4)((-1)^2)((-1)^1) = (-1)^7 = -1.$$

(ii) disjoint cycles so the order is $\text{lcm}[6,5] = 30$ and the sign is $((-1)^5)((-1)^4) = -1$

(iii) disjoint cycles so order is $\text{lcm}[2,2,4,2] = 4$ and sign is $(-1)^{1+1+3+1} = (-1)^6 = 1$

(iv) (12345678)(18765432) not disjoint so we have as disjoint cycles (1)(2)(3)(4)(5)(6)(7)(8) and so order is $\text{lcm}[1,1,1,1,1,1,1,1] = 1$ and sign is 1.

4.2.2 Consider the pair of transpositions (12) and (23) whose product (123) has order 3.

4.2.3 Consider the permutation (12)(34). This has order 2, but is not a transposition.

4.2.4 Assume that $(\pi\sigma)^2 = \pi^2\sigma^2$. Show that $\pi\sigma = \sigma\pi$. Proof: We have $\pi\sigma\pi\sigma = \pi\pi\sigma\sigma$. Multiply (actually compose) with σ^{-1} on the right and π^{-1} on the left to obtain the desired result.

4.2.5 Use the pair of transpositions from 4.2.2 and just compute the powers. Also note that $(23)(12) = (132)$ but $(12)(23) = (123)$ so they don't commute.

4.2.6 First (21463) is a 5-cycle so it has order 5

(12)(345) are disjoint so order is lcm of 2 and 3, i.e. 6

(12)(34) disjoint form so order is lcm $[2, 2] = 2$.

4.2.7 First write as disjoint cycles, then use the lcm of the cycle lengths to get the orders

$(123)(234) = (12)(34)$ so order is $\text{lcm}[2, 2] = 2$

$(123)(324) = (124)(3)$ so order is $\text{lcm}[3, 1] = 3$

$(123)(345) = (12345)$ so order is 5

4.2.9 The set $A(4) = A_4$ is the set of all permuations $\sigma \in S(4)$ which are even, i.e. which have sign equal to 1. Since $|S(4)| = 24$, half of the elements will be even and half will be odd. Thus 12 elements will be even, and these are all listed in the text, with their orders so I won't repeat all of that material here.

4.2.10 I will do this problem in class as it is a fairly hard problem.

4.2.11 In this problem you want to maximize the value of lcm[....] for the given value of n. Thus try to think of writing the elements of $S(n)$ as products of disjoint cycles so as to maximize the lcm value.

In (i) for $S(8)$, the max lcm will be for lcm [5,3] = 15.

In (ii) for $S(12)$, the max lcm will be $\text{lcm}[5, 4, 3] = 60$.

In (iii) for $S(15)$, the max $\text{lcm}[7, 5, 3] = 105$.

Section 4.3

4.3.1 The strategy in these problems is to simply check whether the four axioms (closure, associativity, identity, and inverse) for a group actually hold for all of the

elements in the particular setting.

(i) Rational numbers do not form a group under mul. as there is no inverse under mul. for the 0 element.

(ii) nonzero complex numbers under mul. yes, they form a group

(iii) nonzero integers under mul. - no, because integers don't have inverses in the set of integers

(iv) all functions from $\{1, 2, 3\}$ to itself do not form a group becasue not all functions have inverses. Remember only those functions which are 1-1 and onto will have inverses.

(v) under addition, real numbers of the form $a + b\sqrt{2}$ where a and b are integers. Yes, this is a group. The element $0 + 0\sqrt{2}$ will be the identity, and it is closed because

$(a + b\sqrt{2}) + (c + d\sqrt{2}) = (a + c) + (c + d)\sqrt{2})$.

(vi) under matrix mul., all 3×3 matrices of the given form. Yes, mul. together two matrices of this form and you will get another matrix of that same form so the operation is closed. You check the other properties.

(vii) set of integers under subtraction - no, not a group because subtraction is not associative

For example $(1 - 2) - 3 = -1 - 3 = -4$, but $1 - (2 - 3) = 1 - (-1) = 1 + 1 = 2$

(viii) real numbers with an operation $a * b = a + b + 2$. This is a group. For example, the identity is the element -2 since $a*(-2) = a+(-2)+2 = a$. The inverse of an element a is the element $-4-a$; because $a*(-4-a) = a+(-4-a)+2 = -2$.

4.3.2 Show that in a group $(ab)^{-1} = b^{-1}a^{-1}$. Thus the inverse of a product is the product of the inverses but in the reverse order. Recall this is what happened with the inverse of a composition of two functions, and the reason is that permutations will shortly form a group and thus must obey this property!!!

$(ab)(ab)^{-1} = abb^{-1}a^{-1} = e$

and $(ab)^{-1}(ab) = b^{-1}a^{-1}ab = e$.

4.3.3 Show that if $a^2 = e$ for every $a \in G$ a group, then G is abelian. We have $(ab)^2 = (ab)(ab) = e$ so now multiply on the left by a^{-1} and on the right by b^{-1} so we are left with $ba = a^{-1}b^{-1} = ab$ and we are done. Notice in the last step I have replaced the inverses of a and b by just a and b themselves, but this is a valid step since if $a^2 = e$, then $a^{-1} = a$, and of course similarly for the element b.

4.3.4 A hint here is to show that for the new operation *, the identity under * is $e = ci$ where i is the identity for the original operation in G. Recall that if i is the identity for the old operation in G, then $ci = ic$.

4.3.5 Let A be the three by three matrix in which every entry is a and let X be the three by three matrix in which every entry is say b. Then calculate the matrix product AX which will then force $a = 1/3$.

4.3.8 The answer in the text is correct, but it is not unique. There are other ways to complete the table. The main strategy that I used to get a solution is to view c as the identity for the group. This will enable you to complete a number of vacant positions.

Section 4.4

Section 5.1

5.1.1 Show $ab = ba$ in a group if and only if $(ab)^{-1} = a^{-1}b^{-1}$. We have $(ab)a^{-1}b^{-1} = e$ so by multiplying on the right by b we obtain $aba^{-1} = b$ and now multiply on the right again but now multiply by a and we are done.

5.1.2 Working in a group, solve $axba^{-1} = b$ for x. Multiply on the left by a^{-1} to obtain $xba^{-1} = a^{-1}b$; now multiply on the right by a to get $xb = a^{-1}ba$ and finally multiply on the right by b^{-1} to get $x = a^{-1}bab^{-1}$. In this kind of problem just be careful that things don't commute so you have to multiply very carefully on one side or the other.

5.1.3 See the solution in the text.

5.1.4 (i) subgroup

(ii) not a subgroup because the oeration in the big group is addition but the operation in the subset is multiplication.

(iii) not closed; for example $(12)(13) = (132) \notin$ the set.

5.1.5 See the example in the text.

5.1.6 See the text

5.1.7 Let $x^m \in H$ with m the smallest such value. Let $h \in H$ be arbitrary. But since $h \in G$, we have $h = x^k$ for some k. By the Division Algorithm write $k = mK + r$, with $0 \leq r < m$. Then $h = x^k = x^{mK+r} = x^{mK}x^r$ which implies that $x^r \in H$. But m was the smallest such value so $r = 0$. Then $h = x^k = (x^m)^K$ so h is a power of x^m and we are done.

5.1.8 Use induction on k. For $k = 1$ we have $g^{-1}xg = g^{-1}xg$ so it works for $k = 1$. For k assume that $(g^{-1}xg)^k = g^{-1}x^kg$. Then for $k + 1$ we have

$$(g^{-1}xg)^{k+1} = (g^{-1}xg)(g^{-1}xg)^k = g^{-1}xg(g^{-1}x^kg) = g^{-1}x^{k+1}g$$

and we are done.

5.1.9 aRb if $b = g^{-1}ag$ for some $g \in G$.

Ref. $a = e^{-1}ae$ so yes

Sym. If $b = g^{-1}ag$ then $gb = ag$ and so $gbg^{-1} = a = (g^{-1})^{-1}bg^{-1}$ so sym.

Trans. If $b = g^{-1}ag$ and $c = h^{-1}bh$ then $c = h^{-1}bh = h^{-1}g^{-1}agh = (gh)^{-1}a(gh)$ and so trans. holds.

5.1.10 In Z_{23}^* the element 5 has order 22. Recall the order must divide $\phi(23) = 22$, so check that the order of 5 is not 1, 2, or 11 and you are done.

In Z_{26}^* the element 7 works. Again the order must divide $\phi(26) = 12$ so show that 7 has order 12 by showing it's order is not 1, 2, 3, 4, or 6.

$G_8 = Z_8^* = \{1, 3, 5, 7\}$ is not cyclic as the order of 1 is one, and the orders of

3,5,7 are all two, not four which would be needed if G_8 was cyclic.

Section 5.2

5.2.1 The subgroup $H = \{1, 13\}$. Hence in addition to the coset H itself, the cosets are given by $3H = \{3, 11\}$, and $5H = \{5, 9\}$.

5.2.2 Write $n = p_1^{e_1} \dots p_r^{e_r}$ where the p_i are distinct primes. If n is odd then the result is easy because $\phi(p_i) = p_i^{e_i} - p_i^{e_i - 1} = p_i^{e_i - 1}(p_i - 1)$ is even and hence the product $\phi(n)$ will be even.

Assume now that n is even, so we may assume that $p_1 = 2$. Hence unless $e_1 = 1$, $\phi(2^{e_1}) = 2^{e_1 - 1})$ is even and we are done.

5.2.4 Let H be a subgroup of G and let $a \in G$. Let $b \in aH$ so that $b = ah$ for some $h \in H$. Then we have

$$\{b^{-1}c | c \in aH\} = \{(ah)^{-1}c | c \in aH\} = \{h^{-1}a^{-1}c | c \in aH\}$$

$$= \{h^{-1}a^{-1}ak | k \in H\} = \{h^{-1}k | k \in H\} = \{k | k \in H\} = H.$$

5.2.5 $\phi(20) = 2(4) = 8$ so the possible orders must divide 8 by Lagrange's theorem and hence the possibilities are 1,2,4,8.

However we have

a order (a)

1 1

3 4

7 4

9 2

11 2

13 4

17 4

19 2

Hence there is no element of order 8, thus no subgroup of order 8. Thus in a finite group G there may not be a subgroup of every order dividing the order of the group G.

Section 5.4

5.4.2 In each part calculate the minimum distance of the code; remembering that a code can correct k errors if the minimum distance of the code is at least $2k+1$, and it can detect k errors if the minimum distance of the code is at least $k+1$.

Using these facts, the first two codes can detect one error, but not detect any. The third code correct one and detects two errors, and the last code corrects none and detects none.

5.4.3 See the solution in the text.

5.4.4 The entire decoding table is given in the text so I won't repeat it here.

5.4.5 See the solution in the text. First find the parity-check matrix H for the code from the generator matrix given on page 247. Then calculate the syndrome for each received vector

5.4.6 See the solution in the text. Calculate the syndrome for each coset leader.

5.4.7 See the solution in the text. This is very similar to problem 5.4.6.