Mathmatics 239 solutions to Homework for Chapter 7

35.4, 36.11, 36.15, 37.3, 36.14 (valued as five questions), E-primes

§35.4 a. Suppose $a < b$. Then $a \mod b = a$ because a is a good remainder. On the other hand, $b \mod a < a$ by the definition of remainder. This contradicts them being equal. The same happens when $b < a$ by switching letters.

b. Suppose $a < b$. Then $a \text{ div } b = 0$ because a is already a good remainder, positive and less than b. On the other hand $b \text{ div } a \geq 1$ because $0 < b - a$, so we can subtract at least one copy of a. This contradicts them being equal. The same happens when $b < a$ by switching letters.

EXTRA §35.6 Negative divisors. For normal division we require $0 \leq r < b$. This makes no sense if $b \leq 0$. We know and understand that division by zero has problems. There are some choices for negative division, I will prove the following:

Let $a, b \in \mathbb{Z}$ with $b < 0$. There exist unique integers q and r such that $a = qb + r$ and $0 \leq r < |b|$.

follow along the proof of 35.1 Here we go . . .(please read along in the book)

Let a and b be integers with $b < 0$. The first goal is to show that the quotient and remainder exist; that is there exist integers q and r that satisfy the two conditions $a = qb + r$ and $0 \leq r < |b|$.

Let $A = \{a - bk \mid k \in \mathbb{Z}\}$

We want the remainder to be nonnegative, so we consider only the nonnegative elements of A. Let $B = A \cap \mathbb{N} = \{a - bk \mid k \in \mathbb{Z}, a - bk \geq 0\}$

We want to select the least element of B. Note that the Well-Ordering Principle applies to nonempty subsets of $\mathbb{N}$. Thus we need to check that $B \neq \emptyset$. As long as $k > \frac{a}{b}$ (notice the change of the inequality because $b < 0$), then $a - kb \in B$, so it is nonempty. Since $B \neq \emptyset$, by the Well-Ordering Principle, we can choose $r = a - bq$ to be the least element in B. We may rewrite to $a = qb + r$. Since $r \in B \subset \mathbb{N}$, we also know that $r \geq 0$. We still need to show that $r < |b|$. To prove this, suppose, for the sake of contradiction, that $r \geq |b|$. This means we can still add another b to r without making a negative result. We have $r = a - qb \geq |b| = -b$. Let $r' = r + b = (a - qb) + b \geq 0$, so $r' = (a - qb) + b = a - bq + b = a - (q - 1)b \geq 0$. Therefore $r' \in B$ and $r' = r + b < r$. This contradicts the fact that r is the smallest element of B. Therefore $r < |b|$ as desired.

Now to uniqueness.

Suppose, for the sake of contradiction, there are two different pairs of polynomials, (q, r) and (q', r') that satisfy the conditions of the theorem, that is,

$a = qb + r$ with $0 \leq r < |b|$ and

$a = qb' + r'$ with $0 \leq r' < |b|$.

Combining the two equations on the left gives $qb + r = q'b + r'$ so $r - r' = (q' - q)b$ This means that $r - r'$ is a multiple of b. But recall that $r, r' < |b|$. The difference of the two numbers can be at most $-b - 1$. The only way $r - r'$ can be a multiple of b is if it is zero. This says $r - r' = 0$, so $r = r'$ and $(q - q')b = 0$. Since $b \neq 0, q - q' = 0$, so $q = q'$. Therefore the pairs are not different and we have a contradiction, thus proving uniqueness.

EXTRA §35.9 Prove that the sum of any three consecutive integers is divisible by 3.

This question seems strangely out of context, but we'll try. Consecutive integers could be $a, a+1, a+2$. Their sum is $3a+3 = 3(a+1)$, so is divisible by 3.

EXTRA §35.12 Polynomial division. Great preview for 301 for those secondary-ed students.

(a) $p \mid q$ if there exists a polynomial (with rational coefficients), d, such that $pd = q$.
See: $(2x-6)\left(\frac{1}{2}x^2 + \frac{3}{2}\right) = x^3 - 3x^2 + 3x - 9$

(b) $2x-6 \mid x-3$ and $x-3 \mid 2x-6$ but $x-3 \neq 2x-6$

(c) Two polynomials that divide each other are constant rational multiples. Of interest, as polynomials $6 \mid 2$, even though as numbers it is not true that $6 \mid 2$.

(d) - (e) follow along the proof of 35.1 Here we go again. . .(please read along in the book, or above, if you prefer)

Let a and b be polynomials with $b \neq 0$. The (d) goal is to show that the quotient and remainder exist; that is there exist polynomials q and r that satisfy the two conditions $a = qb + r$ and $\deg r < \deg b$.

Let $A = \{a - bk \mid k \text{ a polynomial with rational coefficients}\}$

Polynomials aren't well ordered, but their degrees are so we also consider

$B = \{\deg(a - bk) \mid k \text{ a polynomial with rational coefficients}\}$

We want to find the k that produces the minimal element of B. Note that B is a subset of $\{-1\} \cup N$. It is nonempty because A is and polynomials all have degrees. $-1 \cup N$ is well ordered because N is and we say $-1 < n$ for all natural n. We can choose $r = a - bq$ to produce the least degree in B, where q is a polynomial with rational coefficients. We may rewrite to $a = qb + r$. We still need to show that $\deg r < \deg b$. To prove this, suppose, for the sake of contradiction, that $\deg r \geq \deg b$. We think about what we would do if we had this problem and we were doing long division. We multiply b by something like cx^n so that r and $cx^n b$ have the same highest term. Then we subtract to get $r' = r - cx^n b$ which has canceled the leading term. So, $\deg r' < \deg r$. But $r' = r - cx^n b = a - bq - cx^n b = a - (q + cx^n)b$. This says that r' is in A, but it has smaller degree than r. This is a contradiction. Therefore $\deg r < \deg b$ as desired.

Now to (e) and uniqueness.

Suppose, for the sake of contradiction, there are two different pairs of polynomials, (q, r) and (q', r') that satisfy the conditions of the theorem, that is,

$a = qb + r$ with $\deg r < \deg b$ and

$a = qb' + r'$ with $\deg r' < \deg b$.

Combining the two equations on the left gives $qb + r = q'b + r'$ so $r - r' = (q' - q)b$ This means that $r - r'$ is a multiple of b. But recall that $\deg r, \deg r' < \deg b$. The difference $r - r'$ is a polynomial with degree less than or equal to that of both r and r', so $\deg(r - r') \leq \deg r < \deg b$. The only way a multiple of b can have lesser degree is if it is zero. This says $r - r' = 0$, so $r = r'$ and $(q - q')b = 0$. Since $b \neq 0, q - q' = 0$, so $q = q'$. Therefore the pairs are not different and we have a contradiction, thus proving uniqueness.

§36.11 Prove that consecutive integers must be relatively prime.

Let x be the lower of two consecutive integers. Then the second is $x+1$. Suppose that $d = \gcd(x, x+1)$. By definition of greatest common divisor, $d \mid x$ and $d \mid x+1$, therefore $d \mid (x+1) - x$, i.e. $d \mid 1$. We know that $1 \mid x$ and $1 \mid x+1$ and that $d \mid 1$. Therefore 1 is the greatest common divisor. Hence, x and $x+1$ are relatively prime.

§36.15 Suppose a and b are relatively prime and that $a \mid c$ and $b \mid c$. Prove that $ab \mid c$.

Assume a and b are relatively prime and that $a \mid c$ and $b \mid c$. Because a and b are relatively prime, $\gcd(a, b) = 1$. Recall that we may write the gcd as a linear combination of the two numbers, therefore there are integers x, y such that $ax + by = 1$. Because $a \mid c$ we have an integer p such that $ap = c$. Because $b \mid c$ we have an integer q such that $bq = c$. Consider $ax + by = 1$ again. Multiply both sides by c to get $cax + cby = c$. Substitute $c = bq$ for the first c and $c = ap$ for the second c. This yields $(bq)ax + (ap)by = c$ Commuting multiplication and factoring we get $ab(qx + py) = c$. Therefore $ab \mid c$.

EXTRA §36.21 13 and 8 are relatively prime, therefore there exist integers x and y such that $13x+8y = 1$. Either by inspection or the Euclidean algorithm we see $13(5)+8(-8) = 1$. So we may first fill 5 of the 13 ounce cups, and then remove 8 of the 8 ounce cups to get 1 ounce.

If a and b are relatively prime, we may duplicate this feat. The equation $ax + by = 1$ instructs us how to add and remove liquid. This condition is necessary because if we can manipulate the cups in this way we can determine a number of each to add or remove, and then find x and y such that $ax + by = 1$ which implies that a and b are relatively prime.

§37.3 Solve the following equations for x.

(a) $2 \otimes x = 4$ in $\mathbb{Z}_{10}$.

Review the multiplication table on p. 270. Look across the 2 row. See that $2 \otimes 2 = 4$ and $2 \otimes 7 = 4$. Therefore the solution is $\{2, 7\}$.

(b) $2 \otimes x = 3$ in $\mathbb{Z}_{10}$.

Looking across the 2 row again, we notice there are no products equal to 3. Therefore the solution is $\emptyset$.

Let's derive a multiplication table for $\mathbb{Z}_{12}$ (it seems a handy thing to do, though we only need the 9 row for these questions)

$\otimes$	0	1	2	3	4	5	6	7	8	9	10	11
0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9	10	11
2	0	2	4	6	8	10	0	2	4	6	8	10
3	0	3	6	9	0	3	6	9	0	3	6	9
4	0	4	8	0	4	8	0	4	8	0	4	8
5	0	5	10	3	8	1	6	11	4	9	2	7
6	0	6	0	6	0	6	0	6	0	6	0	6
7	0	7	2	9	4	11	6	1	8	3	10	5
8	0	8	4	0	8	4	0	8	4	0	8	4
9	0	9	6	3	0	9	6	3	0	9	6	3
10	0	10	8	6	4	2	0	10	8	6	4	2
11	0	11	10	9	8	7	6	5	4	3	2	1

(c) $9 \otimes x = 4$ in $\mathbb{Z}_{12}$.

Looking across the 9 row, we notice there are no products equal to 4. Therefore the solution is $\emptyset$.

(d) $9 \otimes x = 6$ in $\mathbb{Z}_{12}$.

Looking across the 9 row again, we find that $9 \otimes 2 = 6$, $9 \otimes 6 = 6$, and $9 \otimes 10 = 6$. Therefore the solution is $\{2, 6, 10\}$.

EXTRA §37.10 If p is prime, $a \otimes b = 0$ if and only if $a = 0$ or $b = 0$ in $\mathbb{Z}_p$.

Suppose p is prime. Proving the simple direction first. Suppose $a = 0$, then $0 \otimes b = 0$. Suppose $b = 0$, then $a \otimes b = 0$. Therefore if $a = 0$ or $b = 0$, then $a \otimes b = 0$.

Conversely, suppose $a \otimes b = 0$ and for the sake of contradiction that $a \neq 0$ and $b \neq 0$. Since p is prime, and $a \in \mathbb{Z}_p$, we have a relatively prime to p, therefore a is invertible. We will multiply both sides of $a \otimes b = 0$ by the inverse to produce $b = 0$, which is a contradiction. Therefore $a = 0$ or $b = 0$, as desired.

§37.14 (a) For $a \in \mathbb{Z}_n$, prove or disprove $a^b = a^{b \bmod n}$. Let $n = 4, b = 5, a = 2$. $a^b = 2^5 = 2 \otimes 2 \otimes 2 \otimes 2 = 0 \otimes 2 \otimes 2 = 0$.

On the other hand, $a^{b \bmod n} = 2^{5 \bmod 4} = 2^1 = 2$.

Therefore we have that $a^b \neq a^{b \bmod n}$. The statement is false in general.

(b) Find, in $\mathbb{Z}_{100}$, the value of 3^{64}.

$3^{64} = 3(2^6) = (((((3^2)^2)^2)^2)^2)^2 = (((((9)^2)^2)^2)^2)^2 = ((((81)^2)^2)^2)^2 = (((61)^2)^2)^2 = ((21)^2)^2 = (41)^2 = 81$.

(c) Estimate how many multiplications are needed to calculate a^b in $\mathbb{Z}_n$.

Roughly by looking at part (b) we estimate that it takes $\ln_2 b$ steps. This is not quite correct, though. Perhaps this error was within their expectations of "estimate", but to me it seems closer to the sum of the base two logs of the non-zero place values when the number is expressed as a binary numeral. Therefore while a^{64} takes 6 steps, a^{63} would take $5 + 4 + 3 + 2 + 1 = 15$ steps, naively (i.e. this is what I thought). But, if we record our work along the way and remember our answers we don't need to recompute them. Keeping with a^{63}. We take 5 multiplications to compute a^2, a^4, a^8, a^{16}, and a^{32}. And now multiply $a^1 \cdot a^2 \cdot a^4 \cdot a^8 \cdot a^{16} \cdot a^{32}$. This is 5 more mulitplications. So, it takes up to $\ln_2 b$ multiplications to compute all the pieces and up to $\ln_2 b$ multiplications again to put them all togeher. Using this technique we can reduce to $2 \ln_2 b$ computations. This is the best we can hope for. Notice this has nothing to do with $\bmod n$, this is just how many multiplications need to be done to exponentiate.

(d) Give a sensible definition for a^0 in $\mathbb{Z}_n$. Just like with regular exponents, we like the rule $a^n \otimes a^m = a^{n+m}$. Therefore we would want that $a^0 \otimes a^m = a^{0+m} = a^m$. Therefore a^0 should be the multiplicative identity, i.e. $a^0 = 1$.

(e) Give a sensible definition for a^b in $\mathbb{Z}_n$ when $b < 0$.

Using the above rule we would like $a^p \otimes a^{-p} = a^{p+(-p)} = a^0 = 1$. Therefore a^{-p} should be the multiplicative inverse of a^p (if it has one). Therefore we have that a^{-p} will be defined to be $(a^p)^{-1}$, where the outer "-1" means inverse. We can also define, equivalently, a^{-p} to be $(a^{-1})^p$, here where the inner "-1" means inverse. Should you be upset that a^{-1} already has a meaning? No, we should not, because we have sensibly defined these two to agree.

Supplemental questions: Let $E = \{1, 2, 4, 6, 8, \dots\}$. In this set there are some numbers that can only be written as a product of 1 and the number itself, but cannot be written as the product of two other elements of the set. An element of E will be called E-prime if it can only be expressed as a product of 1 and itself. For example, 6 is E-prime since $6 = 1 \cdot 6; 6 = 2 \cdot 3$, but 3 is not in E. An even number will be called E-composite if it is not E-prime. Note: 1 is not a E- prime.

a. Determine the first ten E-primes.

2, 6, 10, 14, 18, 22, 26, 30, 34, 38

There is something to be proven here, namely that these do not have another factorisation. This proof is simple. Because they all have only one two in their prime factorisation

b. Can every E-composite number be factored into a product of E-primes? Justify your reasoning.

Yes. The proof is almost identical to the proof we did in class for the fact that every composite number can be factored into a product of primes.

The proof is by strong induction on n. We prove that for every E-composite number n, it can be factored into a product of E-primes. In fact, we'll prove more, because its easier to do so (one of those tricky cases). We'll prove that every element of E can be factored into E-primes.

Base cases: 1 is the empty product of E-primes and every E-prime is its own E-prime factorisation.

Induction step: Suppose every E number $k < n$ can be factored into E-primes.

Goal: Prove that the E number n can be factored into E-primes.

Because we've proven this already for all E-primes, n is E-composite. Therefore, it can be factored into two elements of E, call them x and y, neither of which is 1. Because neither of them are 1, both of them are less than n. Therefore the induction hypothesis applies and each of them can be factored into E-primes. To find the factorisation of n, therefore, multiply the factors of x and y together. The proof is complete.

c. List several even numbers that have only one factorization into E-primes.

4, 8, 12, 16, 20, 24, 28, 32

Again, there is something to be proven here, namely that these do not have another E-prime factorisation. This proof is equally simple. Considering their traditional unique prime factorisation, we see that each of these numbers has at most one odd prime factor. Because all the E-primes are even with one two in their prime factorisation, finding a E-prime factorisation of a number amounts to listing the twos to indicate the number of factors, and then mulitplying the odd factors by the twos. If there is at most one odd factor, this factorisation is hence unique up to order.

d. Find an even number whose E-prime factorization is not unique, that is, an even number that can be factored into products of E-primes in at least two different ways.

Based on the above discussion about what made the unique ones unique, we can find non- unique ones as well:

$36 = 2 \cdot 18 = 6 \cdot 6$

$60 = 2 \cdot 30 = 6 \cdot 10$

$360 = 2 \cdot 2 \cdot 90 = 2 \cdot 18 \cdot 10 = 2 \cdot 6 \cdot 30 = 6 \cdot 6 \cdot 10$ (and I'm not certain that's all - I'll give the first person an extra 4 points on this HW set to either show me another factorisation or prove that that's all).

Note: this is the point of the whole supplement. This is a system where prime factorisation exists, but is not unique. Of further interest, it is curious that while it is not unique, the number of factors that a number has is uniquely determined.

e. Determine a test to decide whether an even number is E-prime.

We have one already in a., factor the number into primes and check the number of twos. If there is one, then it is E-prime. If more, then not. Here's two equivalent, easier, tests: Divide the number by 2, if it is odd it is E-prime, if it is even it is not. This is the only important part of the first test, not much to explain here (given the explantion in part a or something like it). One more test. $n \equiv 2 \mod 4$ iff n is E-prime. Not really very different from the others. More concise to say. More fun with definitions to prove. Let's do it:

Let's do this direction first (ok, I admit, I'm unlikely to do the second direction - they should be identical in reverse): If n
$equiv2 \mod 4$ then n is E-prime.

Suppose $n \equiv 2 \mod 4$. Therefore $4 \mid 2 - n$. So there is an integer k such that $2 - n = 4kn = -4k + 2n2 = -2k + 1 = 2(-k) + 1$ which is an odd number by definition.

Therefore by the second test, n is an E-prime.

More Extra Problems

1. Compute $\gcd(3913, 23177)$ First we'll switch the order. Then division gives us the following equations:

$$23177 = 5 \cdot 3913 + 3612$$

$$3913 = 1 \cdot 3612 + 301$$

$$3612 = 12 \cdot 301$$

So, the greatest common divisor is 301. Working backwards we get

$$301 = 3913 - 3612$$

$$301 = 3913 - (23177 - 5 \cdot 3913$$

$$301 = 6 \cdot 3913 - 1 \cdot 23177$$

A linear combination as desired. Big numbers but not so scary. Imagine finding all the factors, though.

2. Suppose a and p are relatively prime. Before this, prove a lemma:

$$(x + y)^p \equiv x^p + y^p \mod p$$

for any x, y, and p prime (this is that which calculus students always hope is true). By the binomial theorem, $(x + y)^p = \sum_{k=0}^{p} \begin{pmatrix} p \\ k \end{pmatrix} x^{p-k} y^k$. But, for $k \neq 0$ or $p, p \mid \begin{pmatrix} p \\ k \end{pmatrix} = \frac{p!}{(p-k)!k!}$

because all terms in the denominator are less than p, so nothing will cancel the p in the numerator that begins $p!$. Because $p \mid \binom{p}{k}$, the terms except $k = 0$ and $k = p$ will not contribute $\mod p$. So we are left with $x^p + y^p$, as claimed.

We will prove $a^{p-1} \equiv 1 \mod p$ by induction on a.

Base case: $1^{p-1} = 1$, exactly, so also true $\mod p$.

Induction step: Suppose $k^{p-1} \equiv 1 \mod p$. What is $(k+1)^p$? By the lemma it is $k^p + 1^p$ and by the induction hypothesis (and this base case) this is $k + 1 \mod p$, as desired.

3. Prove that $15 \mid 11n^8 + 4n^4$. I will prove separately that $3 \mid 11n^8 + 4n^4$ and that $5 \mid 11n^8 + 4n^4$.

First working $\mod 3$, $11n^8 + 4n^4 \equiv -n^8 + n^4 \mod 3$. Now we have two cases - either n is relatively prime to 3 or it isn't. If it isn't $n = 3k$ and clearly the entire side is divisible by 3. If it is we can apply 2. For the case $p = 3$ this gives $n^2 \equiv 1 \mod 3$ so we find $11n^8 + 4n^4 \equiv -n^8 + n^4 \equiv -1 + 1 \equiv 0 \mod 3$, as desired.

Now working $\mod 5$, $11n^8 + 4n^4 \equiv n^8 - n^4 \mod 5$. Again, if $n = 5k$ the result follows. What if not? Then $n^4 \equiv 1 \mod 5$ and we find $11n^8 + 4n^4 \equiv n^8 - n^4 \equiv 1 - 1 \equiv 0 \mod 5$, as desired.