UMASS AMHERST MATH 300 FALL '05, F. HAJIR

SOLUTIONS FOR HOMEWORK 6: NUMBER THEORY

1. Problems

1. Suppose $a, b, c \in \mathbb{Z}$.
(a) Show that if $a|b$ and $c \neq 0$, then $ca|cb$.

If $a|b$, then $ax = b$ for some $x \in \mathbb{Z}$, so $cax = cb$ so $(ca)x = (cb)$ i.e. $ca|cb$.

(b) Show that if $a|b$ and $b|c$, then $a|c$.

If $ax = b$ and $by = c$ with $x, y \in \mathbb{Z}$, then $(ax)y = c = a(xy)$ so $a|c$ since $xy \in \mathbb{Z}$.

(c) Show that if $a|b$ and $a|c$, then $a|(mb + nc)$ for all $m, n \in \mathbb{Z}$.

If $ax = b$ and $ay = c$ with $x, y \in \mathbb{Z}$, then $mb+nc = max+nay = a(mx+ny)$ so $a|(mb+nc)$ since $mx + ny \in \mathbb{Z}$.

2. Show that there are arbitrarily long sequences of consecutive integers containing no primes. In other words, show that given an integer $N \geq 1$, there exists an integer a such that $a + 1, a + 2, \ldots, a + N$ are all composites. Hint: try $a = (N + 1)! + 1$. Look for an "obvious" divisor of $a + 1$, an "obvious" divisor of $a + 2$ etc.

With $a = (N + 1)! + 1$, we have $2|2$ and $2|(N + 1)!$ so $2|(a + 1)$ by Problem 1. Indeed, for $2 \leq j \leq N + 1$, $(N + 1)! + j = a + (j - 1)$ is divisible by j because $j|j$ and $j|(N + 1)!$. On the other hand, clearly each such j satisfies $2 \leq j < a + (j - 1)$ so $a + (j - 1)$ cannot be a prime, hence must be composite.

3. Suppose a, b, n are integers, $n \geq 1$ and $a = nd + r$, $b = ne + s$ with $0 \leq r, s < n$, so that r, s are the remainders for $a \div n$ and $b \div n$, respectively. Show that $r = s$ if and only if $n|(a - b)$. [In other words, two integers give the same remainder when divided by n if and only if their difference is divisible by n.]

Suppose $r = s$. Then $r = s = a - nd = b - ne$. Rearranging the last two equalities, we get $a - b = nd - ne = n(d - e)$ so $n|(a - b)$. Conversely, suppose $n|(a - b)$; we will prove that then $r = s$ by contradiction. If $r \neq s$, then switching r, s if necessary, we can assume without loss of generality that $r > s$. By assumption, $n|(a - b)$. Thus, $nx = a - b$ for some $x \in \mathbb{Z}$ so

$$a - b = nd + r - ne - s = n(d - e) + r - s = nx.$$

Rearranging the last equality we have $r - s = n(d - e - x)$ and $d - e - x \in \mathbb{Z}$ so $n|(r - s)$. Since $r > s$, we conclude that $r - s \geq n$ because the least positive multiple of n is n itself. But we have $0 \leq s < r < n$ so $r - s < n$, a contradiction. We have thus shown that $r = s$ if $n|(a - b)$.

4. If $n \geq 2$ and $m_1, \cdots, m_n \in \mathbb{Z}$ are n integers whose product is divisibe by p, then at least one of these integers is divisible by p, i.e. $p|m_1 \cdots m_n$ implies that then there exists $1 \leq j \leq n$ such that $p|m_j$. Hint: use induction on n.

Proof by induction on n. Base case $n = 2$ was proved in class and in the notes as a consequence of Bézout's theorem.

Induction step. Suppose $k \geq 2$ is an integer such that whenever we are given k integers $m_1, \ldots, m_k \in \mathbb{Z}$ whose product is divisible by p (i.e. $p|(m_1 \cdots m_n)$), there exists $1 \leq j \leq k$ such that $p|m_j$. Now suppose we are given $k + 1$ integers $m_1, \ldots, m_{k+1}$ such that $p|(m_1 \cdots m_{k+1})$. We have $p|mm_{k+1}$ where $m = m_1 \cdots m_k$. By the base case, we conclude that either $p|m$ or $p|m_{k+1}$. If $p|m_{k+1}$, then certainly there exists $1 \leq j \leq k + 1$ such that $p|m_j$, namely $j = k + 1$. Otherwise, $p|m$ and by the induction hypothesis, then there exists $1 \leq j \leq k$ such that $p|m_j$. Thus, we have shown that there exists $1 \leq j \leq k + 1$ such that $p|m_j$, completing the induction step. By PMI, we are done.

5. (a) Calculate $\gcd(315, 168)$ using the Euclidean algorithm, then use this information to calculate $\text{lcm}(315, 168)$. Determine integers x, y such that $315x + 168y = \gcd(315, 168)$. You may use the Blankinship version of the Bezout algorithm if you wish. Now obtain the prime factorizations of 315 and 168 to double-check your computation of the gcd and lcm of 315 and 168.

To find $\gcd(315, 168)$, we perform the Euclidean algorithm, keeping track of what it does to the two extra columns comprising an "identity" matrix.

$$\begin{array}{rrr} 315 & 1 & 0 \\ 168 & 0 & 1 \\ 147 & 1 & -1 \\ 21 & -1 & 2 \\ 0 & 8 & -15. \end{array}$$

We read off that $\gcd(315, 168) = 21$ (the last non-zero remainder) and that $-1(315) + 2(168) = 21$. We also have $8(315) - 15(168) = 0$ i.e. $8(315) = 15(168)$ and that $\text{lcm}(315, 168) = 8(315) = 15(168) = 2520$. Or we could use $\text{lcm}(315, 168)\gcd(315, 168) = 315 \cdot 168$.

To double-check, we have $315 = 3^2 \cdot 5 \cdot 7$ and $168 = 2^3 \cdot 3 \cdot 7$, so $\gcd(315, 168) = 3 \cdot 7$ and $\text{lcm}(315, 168) = 2^3 \cdot 3 \cdot 5 \cdot 7$.

(b) Calculate $\gcd(89, 148)$ using the Euclidean algorithm.

$$\begin{array}{rrr} 148 & 1 & 0 \\ 89 & 0 & 1 \\ 59 & 1 & -1 \\ 30 & -1 & 2 \\ 29 & 2 & -3 \\ 1 & -3 & 5 \\ 0 & 89 & -148. \end{array}$$

Thus, $\gcd(148, 89) = 1$.

6. (a) Show that if $n > 1$ is composite, then there exists d in the range $1 < d \leq \sqrt{n}$ such that $d|n$. (Hint: you might want to use proof by contradiction).

Proof by contradiction. Suppose for all d in the range $1 < d \leq \sqrt{n}$, d does not divide n. In other words, all divisors of n greater than 1 are in fact greater than $\sqrt{n}$. Since n is composite, there exists an integer e in the range $1 < e < n$ such that $e|n$. Then $ef = n$ for some integer f. Since f is also a positive divisor of n, it follows from our assumption that $e > \sqrt{n}$ and $f > \sqrt{n}$. (Note that we cannot have $f = 1$ because $e < n$ and we cannot have $f = n$ because $e > 1$). But then $n = ef > \sqrt{n}\sqrt{n} > n$ is a contradiction. Thus, if $n > 1$ is composite, it must admit a divisor in the range $[2, \sqrt{n}]$.

(b) Use (a) to show that if $n > 1$ is not divisible by any integers in the range $[2, \sqrt{n}]$, then n is prime.

Suppose $n > 1$ is not divisible by any integers in the range $[2, \sqrt{n}]$. If n were composite, then by (a), it would have a divisor in this range, so n must be prime.

(c) Use (b) to show that if n is not divisible by any **primes** in the range $[2, \sqrt{n}]$, then n is prime.

Proof by contradiction. Suppose $n > 1$ is not divisible by any primes in the range $[2, \sqrt{n}]$, and that n is composite. By (a), n is divisible by some integer $d \in [2, \sqrt{n}]$. Since every integer > 1 is divisible by at least one prime, there exists a prime $p|d$, so of course $p|n$ since $d|n$. Since $d \in [2, \sqrt{n}]$ and $2 \leq p \leq d$, we have $p \in [2, \sqrt{n}]$ is prime and divides n, a contradiction. This completes the proof.

(d) Use the procedure in (c) to verify that 229 is prime.

We check that $229/p$ for $p = 2, 3, 5, 7, 11, 13$ gives non-zero remainder. Since $\sqrt{229} < 17$, we are done by (c).

(e) Suppose you write down all the primes from 2 to n. We know that 2 is a prime so we circle it and cross out all other multiples of 2. The next uncrossed number is 3 and we claim that 3 therefore must be prime. Explain why. Now cross out all the multiples of 3. The next uncrossed number is 5 so we claim it must be a prime. We continue in this fashion until we get to $\sqrt{n}$. Explain why all the remaining numbers are prime. Carry out this procedure for

$n = 100$ to find all the primes less than 100. This is called the Eratosthenes sieve. (You may want to write them in 10 rows of 10 numbers each).

Once we cross out multiples of $2, 3, \ldots, [\sqrt{n}]$, any number that remains does not have a divisor less than or equal to $\sqrt{n}$ so must be prime by (c).

7. (a) Prove that if $n \in \mathbb{N}$, then $\gcd(n, n+1) = 1$.

Suppose $d|n$ and $d|(n+1)$. Then $d|(n+1-n)$ by Problem 1, i.e. $d|1$ so $d = \pm 1$. Thus, $\gcd(n, n+1) = 1$.

(b) Is it possible to choose 51 integers in the interval $[1, 100]$ such that no two chosen numbers are relatively prime? [i.e. is there a subset $S \subset \{n \in \mathbb{N} \mid 1 \leq n \leq 100\}$ with $|S| = 51$ such that $m, n \in S \Rightarrow \gcd(m, n) > 1$?] Prove that your answer is correct. (Hint: If you get stuck, recall that an often useful problem-solving strategy is to attempt a simpler problem first, so think about 6 integers in $[1, 10]$ for example).

Suppose $S \subseteq \{1, 2, 3, \ldots, 100\}$ and $|S| = 51$. I claim there exists $1 \leq n \leq 99$ such that $n \in S$ and $n + 1 \in S$. We can prove this claim by contradiction. Suppose not. Then if we list the elements of S in increasing order as $s_1 < s_2 < \cdots < s_{51}$, we have $s_{k+1} \geq s_k + 2$ for $1 \leq k \leq 50$. Thus, $s_{51} \geq s_1 + 50(2)$. Since $s_1 \geq 1$, it follows that $s_5 1 \geq 101$ a contradiction. Thus, there exists $1 \leq n \leq 99$ such that $n, n+1 \in S$. Then $\gcd(n, n+1) = 1$ by a previous problem. So we cannot have a subset of size 51 in $\{1, 2, 3, \ldots, 100\}$ no two of whose elements are relatively prime.

8. Show that for $n \geq 1$, in any set of $2^{n+1} - 1$ integers, there is a subset of exactly 2^n of them whose sum is divisible by 2^n. (Hint: use ordinary induction on n).

To ease the notation, let us make a definition. If S is a finite subset of $\mathbb{Z}$, let us define $\sigma_S = \sum_{s \in S} s$ to be the sum of its elements. We want to prove, for $n \geq 1$,

$$P(n): \text{ If } S \subset \mathbb{Z} \text{ has size } 2^{n+1} - 1, \text{ then there exists } T \subset S \text{ of size } 2^n \text{ such that } 2^n | \sigma_T.$$

Induction on n. Base case $n = 1$. Given $2^{1+1} - 1 = 3$ integers, say a, b, c, at least 2 of them must have the same parity, by the pigeonhole principle (there are only two possible "parity pigeonholes" namely even and odd, so the three "pigeons" (a, b, c) cannot get three distinct pigeonholes). So, we take two that have the same parity: their sum is even, i.e. is divisible by $2^n = 2$. This takes care of the base case.

Induction step. Suppose $k \geq 1$ is some integer such that the proposition is true for all subsets of $\mathbb{Z}$ of size $2^{k+1} - 1$. Suppose $S \subset \mathbb{Z}$ and $|S| = 2^{k+2} - 1$. We are looking for a subset $T \subset S$ of size 2^{k+1} such that $\sigma_T = \sum_{t \in T} t$ is divisible by 2^{k+1}.

Step 1. Chop Shop. If we set aside a random element, say $x \in S$, we can chop up the rest of S into two subsets S_1, S_2 of equal size, i.e. $\Delta = \{S_1, S_2, \{x\}\}$ is a partition where $|S_1| = |S_2| = (2^{k+2} - 2)/2 = 2^{k+1} - 1$. There are many choices for S_1, S_2, x of course, we just choose any one we like.

Step 2. A tale of two pigeons. By the induction hypothesis, there exist $T_1 \subset S_1$ and $T_2 \subset S_2$ of size $|T_1| = |T_2| = 2^k$ such that σ_{T_1} and σ_{T_2} are divisible by 2^k. It is tempting to

take $T = T_1 \cup T_2$, but then we will have only that 2^k divides σ_T. Namely we have $\sigma_{T_1} = 2^k a$ and $\sigma_{T_2} = 2^k b$ so $\sigma_T = \sigma_{T_1} + \sigma_{T_2} = 2^k(a+b)$. So what is the problem? The problem is that 2^{k+1} divides σ_T if and only if $2|(a+b)$, i.e. if and only if a, b have the same parity. Now, since we have only two numbers, a, b, we can't guarantee they have the same parity! (conclusion: not enough pigeons!) Got to get me some more pigeons by golly.

Step 3. The magical third pigeon. The critical step in this problem is to realize that if we could find another "pigeon" i.e. another subset S_3 of S of size $2^{k+1}-1$, then inside it we can find 2^k elements that add up to something of the form $2^k c$ with $c \in \mathbb{Z}$, then among a, b, c we'll be able to find two of the same parity. BUT, we have already used up the elements of T_1 and T_2 and do not want to disturb them, so we have to make sure that S_3 is disjoint from T_1 and T_2 (i.e. we don't have any "interference" when we add up the sums). If you think about this, then you eventually have the brilliant idea that maybe we should count up how many elements are left outside $T_1 \cup T_2$ to see if we have enough elements left. Well,

$$|S \setminus (T_1 \cup T_2)| = 2^{k+2} - 1 - 2^k - 2^k = 2^{k+2} - 2^{k+1} - 1 = 2^{k+1}(2-1) - 1 = 2^{k+1} - 1!$$

That last "!" is a "surprise" not a "factorial," by the way. In other words, if we gather together **all** the elements we have not yet used up, they form a subset $S_3 = S \setminus (T_1 \cup T_2)$ of size $2^{k+1} - 1$, so we can apply the induction step once again to find a subset $T_3 \subset S_3$ of size $|T_3| = 2^k$ such that $2^k | \sigma_{T_3}$. Now, by construction, T_1, T_2, T_3 are pairwise disjoint. Now, among the three numbers $\alpha_i = \sigma_{T_i}/2^k$, for $i = 1, 2, 3$, by the base case, we are guaranteed two of them add up to an even number, say $\alpha_k + \alpha_l$ is even. Then taking $T = T_k \cup T_l$, we have $|T| = 2^{k+1}$ and $\sigma_T = \sigma_{T_k} + \sigma_{T_l} = 2^k(\alpha_k + \alpha_l)$ so $2^{k+1} | \sigma_T$.

9. Suppose x is a real number such that $x + 1/x$ is an integer. Show that $x^n + 1/x^n$ is also an integer for all $n \geq 1$. (Hint: Use complete induction on n).

To ease the notation, let us put $\alpha = (x + 1/x) \in \mathbb{Z}$ and, for $n \geq 1$, $\alpha_n = x^n + 1/x^n$. The proposition is clearly true for $n = 1$ since $\alpha = \alpha_1$. Let us do $n = 2$ to see what is involved. We have $(x + 1/x)^2 = x^2 + 2 + 1/x^2$, so $x^2 + 1/x^2 = (x + 1/x)^2 - 2$. Thus, if $\in \mathbb{Z}$, then $\alpha_2 = \alpha^2 - 2 \in \mathbb{Z}$ since $\alpha^2 \in \mathbb{Z}$. So there should be some nice relationship between α_n and α^n. Rather, there is a neater relationship between $\alpha\alpha_k$ and α_{k+1}.

Well, let us go to the induction step. We assume, for some integer $k \geq 1$, that $\alpha_j \in \mathbb{Z}$ for $1 \leq j \leq k$. We compute

$$\alpha\alpha_k = (x + 1/x)(x^k + 1/x^k) = x^{k+1} + 1/x^{k-1} + x^{k-1} + 1/x^{k+1}.$$

In other words,

$$\alpha_{k+1} = \alpha\alpha_k - \alpha_{k-1}.$$

By the (complete) induction step, we know that $\alpha_k, \alpha_{k-1} \in \mathbb{Z}$, and certainly $\alpha \in \mathbb{Z}$ so $\alpha_{k+1} \in \mathbb{Z}$.

By the principle of complete mathematical induction, we are done.

10. Here is a "proof" by complete induction that all Fibonacci numbers are even! Your job is to explain the error in the argument.

For $n \geq 0$, let $P(n)$ be the statement that F_n is even. We will prove $P(n)$ by complete induction on n. We check the base case, $P(0)$: $F_0 = 0$ is even. Now we move to the induction step: We must show that if $P(j)$ holds for $0 \leq j \leq n$, then $P(n)$ holds. Well, if $P(j)$ holds

for $0 \leq j \leq n$, then $F_{n+1} = F_{n-1} + F_n$ is even because F_{n-1} and F_n are even by $P(n-1)$ and $P(n)$, respectively. By Complete Induction, therefore, F_n is even for all $n \geq 0$.

The error is in the step where $P(n-1)$ and $P(n)$ are both used. For $n = 1$, this requires both $P(0)$ and $P(1)$ to be true. So, when one wants to do the base case, one needs to check both $P(0)$ and $P(1)$. It is not enough to check $P(0)$. Indeed, when one tries to check $P(1)$, it turns out to be false, for $F_1 = 1$ is odd.