FIRST MIDTERM
MATH 104A, UCSD, AUTUMN 17

You have 80 minutes.

There are 5 problems, and the total number of points is 75. Show all your work. *Please make your work as clear and easy to follow as possible.*

Name:________________________________

Signature:______________________________

Student ID #:___________________________

Section Time:___________________________

Problem	Points	Score
1	15	
2	10	
3	20	
4	10	
5	20	
6	10	
7	10	
Total	75	

1. (15pts) (i) *Give the definition of a prime number.*

A natural number p is prime if $p \neq 1$ and the only divisors of p are 1 and p.

(ii) *Give the definition of the greatest common divisor.*

The greatest common divisor d of two numbers a and b, not both zero, has the following properties:

(1) $d|a$ and $d|b$.
(2) If $d'|a$ and $d'|b$ then $d'|d$.
(3) $d > 0$.

(iii) *Give the definition of a group.*

A group G is a set together with a rule of multiplication which satisfies the following rules:

(1) Multiplication is associative, that is, $a(bc) = (ab)c$ for all a, b and $c \in G$.
(2) There is an identity $e \in G$ such that $ae = a = ea$.
(3) Every element $a \in G$ has an inverse b such that $ab = e = ba$.

2. (10pts) *Show that if* $M_n = 2^n - 1$ *then* M_{rn} *is not prime if* $r > 1$ *and* $n > 1$.

It is straightforward to check the identity

$$a^s - b^s = (a-b)(a^{s-1} + a^{s-2}b + a^{s-3}b^2 + \cdots + b^{s-1}).$$

If we put $a = 2^r$ and $b = 1$ then we get

$$\begin{aligned} M_n &= 2^n - 1 \\ &= (2^r)^s - 1^s \\ &= a^s - b^s \\ &= (a-b)(a^{s-1} + a^{s-2}b + a^{s-3}b^2 + \cdots + b^{s-1}) \\ &= (2^r - 1)k \\ &= kM_r. \end{aligned}$$

Thus M_r divides M_n. As $r > 1$, $M_r > 1$ and as $n > 1$, $M_r \neq M_n$. Thus M_n is not a Mersenne prime.

3. (20pts) (i) *Show that if* $p = 6k + r$ *is prime and* $0 \leq r < 6$ *then either* $p = 2$ *or* $p = 3$ *or* $r = 1$ *or* $r = 5$.

As $0 \leq r < 6$ it follows that $r = 0$, 1, 2, 3, 4 or 5. If $r = 0$, or $r = 2$ or 4 then $p = 2(3k)$ or $p = 2(3k + 1)$ or $p = 2(3k + 2)$ and p is even. In this case $p = 2$. If $r = 3$ then $p = 3(2k + 1)$ is divisible by 3 and $p = 3$. Otherwise $r = 1$ or $r = 5$.

(ii) *Show that the set*

$$S = \{\, 6k + 1 \mid k \in \mathbb{N} \,\}$$

is closed under multiplication.

Suppose that a and $b \in S$. Then we may find k and l such that $a = 6k + 1$ and $b = 6l + 1$. In this case

$$\begin{aligned} ab &= (6k + 1)(6l + 1) \\ &= 36kl + 6k + 6l + 1 \\ &= 6(6kl + k + l) + 1. \end{aligned}$$

Thus $ab \in S$ and S is closed under multiplication.

(iii) *Show that there are infinitely many primes of the form* $6k + 5$.

We use a variation of Euclid's argument. First note that 5 is a prime of the form $6k + 5$. Suppose that there are only finitely many primes, $p_1, p_2, \ldots, p_k$, whose remainder is five when divided by 6.
Let

$$P = \prod_{i=1}^{k} p_i.$$

Note that

$$6P - 1 = 6(P - 1) + 5,$$

has remainder 5 when divided by 6. Consider the prime factorisation of $6P - 1$. As S is closed under multiplication and $6P - 1 \notin S$ it follows that one of the primes in the factorisation has a remainder different fron one, after division by 6.
On the other hand, $6P - 1$ not divisible by 2, 3, or any of the primes $p_1, p_2, \ldots, p_k$, a contradiction. Therefore there are infinitely many primes of the form $6k + 5$.

4. (10pts) (i) *State the fundamental theorem of arithmetic.*

If a is a non-zero integer then a is uniquely a product

$$a = \pm 1 \cdot p_1 \cdot p_2 \dots p_k,$$

where $p_i \leq p_{i+1}$ are primes.

(ii) *Suppose that a, b and c are three integers. Show that if $b|a$, $c|a$ and $(b, c) = 1$ then $bc|a$.*

We may find common prime factorisations

$$a = p_1^{e_1} p_2^{e_2} \dots p_l^{e_l} \qquad b = p_1^{f_1} p_2^{f_2} \dots p_l^{f_l} \qquad \text{and} \qquad c = p_1^{g_1} p_2^{g_2} \dots p_l^{g_l}.$$

As b and c are coprime, it follows that $f_i g_i = 0$ for all i. As $b|a$ it follows that $f_i \leq e_i$. As $c|a$ it follows that $g_i \leq e_i$. But then $f_i + g + i \leq e_i$, since one of f_i and g_i is zero. Thus

$$bc = p_1^{f_1+g_1} p_2^{f_2+g_2} \dots p_l^{f_l+g_l}$$

divides a.

5. (20pts) (i) *Show that if a and b are integers, not both zero, and d is the greatest common divisor, then we may find integers λ and μ such that $d = \lambda a + \mu b$.*

If $a = 0$ then

$$\begin{aligned} d &= b \\ &= 1 \cdot 0 + 1 \cdot b \\ &= 1 \cdot a + 1 \cdot b, \end{aligned}$$

so that we may take $\lambda = \mu = 1$ if $ab = 0$. Note that

$$d = (a, b) = (|a|, |b|).$$

If

$$d = \lambda|a| + \mu|b| \qquad \text{then} \qquad d = (\pm\lambda)a + (\pm\mu)b.$$

Thus we may assume that a and $b > 0$. We may assume that $a \leq b$. If we divide a into b we get

$$b = qa + r \qquad \text{where} \qquad 0 \leq r < a.$$

Note that $\{a, b\}$ and $\{a, r\}$ have the same common divisors, so that

$$d = (a, r).$$

By induction on a we may find integers λ and μ such that

$$d = \lambda a + \mu r.$$

As

$$r = b - qa,$$

it follows that

$$\begin{aligned} d &= \lambda a + \mu r \\ &= \lambda a + \mu(b - qa) \\ &= (\lambda - \mu q)a + \mu b. \end{aligned}$$

This completes the induction and the proof.

(ii) *Show that if p is a prime and $p|ab$ then either $p|a$ or $p|b$.*

If $p|a$ there is nothing to prove and so we may assume that p does not divide a. As the only divisors of p are 1 and p and p does not divide a, it follows that the only common divisor of p and a is 1. Thus the greatest common divisor of p and a is 1. By (i) we may find λ and μ such that

$$1 = \lambda p + \mu a.$$

If we multiply both sides of this equation by b then we get

$$b = \lambda pb + \mu ab.$$

The first term is clearly divisible by p and the second term is divisible by p by assumption. Thus $p|b$.

Bonus Challenge Problems

6. (10pts) *Show that every positive integer can be represented uniquely in the form*

$$F_{n_1} + F_{n_2} + \cdots + F_{n_m},$$

where $m \geq 1$, $n_{j-1} > n_j + 1$, *for* $j = 2, 3, \ldots, m$ *and* $n_m > 1$.

We first prove existence. We proceed by induction on n. If $n = 1$ then we may take $m = 1$ and $n_m = 2$; in this case $1 = F_2$.

Suppose the result is true for all integers up to n. Let n_1 be the largest integer such that $n + 1 - F_{n_1} \geq 0$. Note that $n_1 \geq 2$. If $n + 1 = F_{n_1}$ then we are done. Otherwise, by induction we may find an expression of the form

$$n + 1 - F_{n_1} = F_{n_2} + F_{n_3} + \cdots + F_{n_m},$$

where $m \geq 2$, $n_{j-1} > n_j + 1$, for $3 \leq j \leq m$ and $n_m \geq 2$.

If $n_1 = n_2 + 1$ then

$$\begin{aligned} n + 1 &\geq F_{n_1} + F_{n_1 - 1} \\ &= F_{n_1+1}, \end{aligned}$$

which contradicts our choice of n_1. Thus $n_1 > n_2 + 1$. This completes the induction and the proof of existence.

Now we turn to uniqueness. We first establish that

$$F_n > \sum_{m:1<m<n} F_m$$

where the sum ranges over those integers such that $n - m$ is odd. By induction on n.

If $n = 1$ then there are no integers $1 < m < 1 = n$. Thus the result is true for $n = 1$ for vacuous reasons. Now suppose the result is true for n.

$$\begin{aligned} F_{n+1} &= F_n + F_{n-1} \\ &> F_n + \sum_{m:1<m<n-1} F_m \\ &= \sum_{m:1<m<n+1} F_m. \end{aligned}$$

Here all but the last sum run over integers m such that $n-1-m$ is odd and the last one runs over integers m such that $n + 1 - m$ is odd. Of course both of these parity conditions are the same. Since $n+1-n = 1$ is odd, the last sum includes the index $m = n$.

Suppose that we have two expressions of the form

$$F_{p_1} + F_{p_2} + \cdots + F_{p_m} = F_{q_1} + F_{q_2} + \cdots + F_{q_n},$$

where m and $n \geq 1$, p_m and $q_n > 1$, $p_{i-1} \geq p_i + 2$ and $q_{j-1} \geq q_j + 2$. If there are two indices i and j such that $p_i = q_j$ then we may cancel F_{p_i} and F_{q_j} from both sides. Thus we may that there are no common terms. Possibly switching the sides of the equation, we may assume that $p_1 > q_1$.

$$\begin{aligned} F_{p_1} &> \sum_{m:1<m<p_1} F_m \\ &\geq F_{q_1} + F_{q_2} + \cdots + F_{q_n}, \end{aligned}$$

a contradiction. This proves uniqueness.

7. (10pts) *If n is a natural number then let*

$$p(n) = 1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \cdots + \frac{1}{n}.$$

Show that if $p(n)$ is an integer then $n = 1$.

Let

$$p(n) = 1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \cdots + \frac{1}{n}.$$

Let k be the largest integer such that $2^k \leq n$. Note that no other natural number between 1 and n is divisible by 2^k. Thus if we multiply both sides by 2^{k-1} every term

$$\frac{2^{k-1}}{i} \qquad \text{for} \qquad 1 \leq i \leq n, \qquad i \neq 2^k,$$

of the sum has an odd denominator.

As the sum of rational numbers with an odd denominator, has an odd denominator, it follows that $2^{k-1}p(n)$ is a sum of $1/2$ and a rational number an with odd denominator. In particular $p(n)$ is not an integer.