Math 312, Summer Term 2018
Pre-Midterm Sheet

May 30, 2018

Material

The material for the exam consists of the material covered in the lectures up to and including Wednesday, May 30th, as well as Problem Sets 1 through 3. Here are some headings for the topics we covered (this is not comprehensive)

- Foundations of the natural numbers: well-ordering, proof by induction.
- Foundations of the integers: divisibility and division with remainder.
- The integers: GCD and LCM, Euclid's Algorithm and Bezout's Theorem, primes and unique factorization, irrational numbers. Linear equations.
- Congruences and modular arithemtic: definition of congruence and congruence classes; arithmetic in congruences; invertibility and inverses using Euclid's algorithm; solving congruences. Application: tests for divisibility by 3, 9 and 11.
- Wilson's Theorem, Fermat's Little Theorem, multiplicative order.

Note: the historical discussion of the distribution of primes is not examinable.

Structure

The exam will consist of several problems. Problems can be calculational (only the steps of the calculation are required), theoretical (prove that something holds) or factual (state a Definition, Theorem, etc). The intention is to check that the basic tools are at your fingertips. Generally, earlier problems are easier than latter problems; the number of points a problem is worth should not be used as an indication of difficulty.

Sample problems

Check out the past final exams posted at `http://www.math.ubc.ca/Ugrad/pastExams/index.shtml#312`. Here are a few more problems:

1. (Unique factorization)

   (a) [calculational] Write 148 as a product of prime numbers.

   (b) [factual] State the Theorem on unique factorization of natural numbers.

   (c) [theoretical] Prove that every natural number can be written as a product of primes..

2. Solve the following system of congruences

$$\begin{cases} x + y + z & \equiv 4\,(5) \\ 3x + z & \equiv 1\,(5) \end{cases}$$

3. Prove by induction that $a_n = \frac{n(n+1)}{2}$ is an integer for all $n \geq 0$.

4. (modular arithmetic)

   (a) State the definition of a number invertible modulu m.

   (b) List the invertible residue classes mod 15.

5. (Fermat's Little Theorem) Let p be a prime number.

   (a) Let $1 \leq k \leq p - 1$. Show that $p \mid \binom{p}{k}$.

   (b) Show that $(a + b)^p \equiv a^p + b^p\,(p)$.

   (c) Show by induction on a that for all $a \geq 0$, $a^p \equiv a\,(p)$.

   (d) Conclude that if if $p \nmid a$ then $a^{p-1} \equiv 1\,(p)$.

6. Find the least non-negative residue modulu 73 which is inverse to 10.

7. Let x, y, z be non-negative integers such that $5^x = 6^y + 7^z$.

   (a) Use reduction mod 2 to show that $y \geq 1$.

   (b) Use reduction mod 6 to show that x is even.

   (c) Use reduction mod 5 to show that $z \equiv 2\,(4)$ (in particular $z > 0$)

   (d) Use reduction mod 8 to show that $y \geq 3$.

   (e) (hard) Now show that either $5^{x/2} - 7^{z/2} = 2$ and $5^{x/2} + 7^{z/2} = 2^{y-1} \cdot 3^y$ or $5^{x/2} - 7^{z/2} = 2^{y-1}$ and $5^{x/2} + 7^{z/2} = 2 \cdot 3^y$.

   (f) [not during an exam] Find all solutions to the original equation.

Sample solutions

1. (Unique factorization)

   (a) $148 = 2 \cdot 74 = 2^2 \cdot 37$.

   (b) Every positive integer can be written as a product of primes up, uniquely to reordering the factors [Or: Every positive integer can be uniquely represented by a product $\prod_p p^{e_p}$ over all primes p, where $e_p \in \mathbb{Z}_{\geq 0}$ and all but finitely many are zero).

   (c) Assume that there are natural numbers which cannot be written as a product of primes. Then by the well-ordering principle there is a least such integer which we denote n. Then $n > 1$ (1 is the empty product) and n is not prime (it would be equal to the product containing just itself). n must therefore be composite – assume that $n = ab$ with $1 < a, b < n$. Since both a and b are smaller than n, they can both be written as products of primes. Then n is the product of the two products, a contradiction.

2. Let x, y, z be a solution. From the second congruence we find $z \equiv 1 - 3x\,(5)$, and substituting this into the second we find $x + y + 1 - 3x \equiv 4\,(5)$ so that $y \equiv 3 + 2x\,(5)$. It follows that every solution is of the form $(x, y, z) = (x, 3 + 2x + 5t, 1 - 3x + 5s)$ for some $x, s, t \in \mathbb{Z}$. Conversely, for x, y, z of this form we have $x+y+z = x+3+2x+5t+1-3x+5s = 4+5(s+t) \equiv 4\,(5)$ and $3x + z = 3x + 1 - 3x + 5s = 1 + 5s \equiv 1\,(5)$, so the set of solutions is $\{(x, 3 + 2x + 5t, 1 - 3x + 5s) \mid x, s, t \in \mathbb{Z}\}$.

3. For $n = 0$ we have $a_0 = 0$, which is an integer. We also have $a_{n+1} - a_n = \frac{(n+1)(n+2)}{2} - \frac{n(n+1)}{2} = \frac{n+1}{2}[n + 2 - n] = n + 1$ so that $a_{n+1} = a_n + n + 1$. It follows that if a_n is an integer so is a_{n+1}.

4. (modular arithmetic)

   (a) An integer a is invertible mod m if there is an integer b such that $ab \equiv 1\,(m)$.

   (b) We know that a is invertible mod m iff $(a, m) = 1$, so the invertible residue classes mod 15 are those of $1, 2, 4, 7, 8, 11, 13, 14$.

5. (Fermat's Little Theorem) Let p be a prime number.

   (a) Clearly $p|p!$. On the other hand if $k < p$ then $p \nmid k!$ since p does not divide the factors of $k!$. If $k \geq 1$ then $p - k < p$ so also $p \nmid (n-k)!$. So in $\binom{p}{k} = \frac{p!}{k!(p-k)!}$, p divides the numerator but not the denominator. Since the ratio is an integer it must be divisible by p.

   (b) By the Binomial Theorem, $(a + b)^p = \sum_{k=0}^{p} \binom{p}{k} a^k b^{p-k} = a^p + \sum_{k=1}^{p-1} \binom{p}{k} a^k b^{p-k} + b^p$. We have just seen that $\binom{p}{k} \equiv 0\,(p)$ in for $1 \leq k \leq p - 1$, so we are left with $(a + b)^p \equiv a^p + b^p\,(p)$.

(c) We have $0^p = 0$. Also, by part (b), $(a+1)^p \equiv a^p + 1^p\,(p)$ so if $a^p \equiv a\,(p)$ we have $(a+1)^p \equiv a+1\,(p)$ as claimed.

(d) If $p \nmid a$ then a is invertible mod p. Let $\bar{a}$ be such an inverse. Multiplying both sides of $a^p \equiv a\,(p)$ by $\bar{a}$ we find $a^{p-1} = a^{p-1} \cdot 1 \equiv a^{p-1} a\bar{a} = a^p\bar{a} \equiv a\bar{a} \equiv 1\,(p)$.

6. Following Euclid's algorithm we have $3 = 73 - 7 \cdot 10$ and $1 = 10 - 3 \cdot 3 = 22 \cdot 10 - 3 \cdot 73$. It follows that $22 \cdot 10 \equiv 1\,(73)$, so 22 is inverse to 10 mod 73.. Since $0 \leq 22 < 73$, 22 is the least non-negative residue.

7. Let x, y, z be non-negative integers such that $5^x = 6^y + 7^z$.

(a) 5^x and 7^z are always odd (even if $x = 0$ or $z = 0$). It follows that 6^y is even, while $6^0 = 1$ is odd.

(b) Since $y \geq 1$, 6^y is divisible by 6. Since $5 \equiv -1\,(6)$ and $7 \equiv 1\,(6)$ is follows that $(-1)^x \equiv 1^z = 1\,(6)$. For x odd, $(-1)^x = -1 \not\equiv 1\,(6)$ so x is even.

(c) We cannot have $x = 0$ since the RHS is at least 6, so $5|5^x$. Reducing mod 5 we find $0 \equiv 1^y + 2^z\,(5)$ that is $2^z \equiv -1\,(5)$. Since $2^2 = 4 \equiv -1\,(5)$ while $2^4 = 16 \equiv 1\,(5)$ the order of 2 mod 5 is 4 (if not 4 is would be a divisor but we ruled out 2). Since 2 has order 4 mod 5 and $2^2 \equiv -1\,(5)$ we have $7^y \equiv -1\,(5)$ iff $y \equiv 2\,(4)$.

(d) Mod 8 we have $5^2 = 24 + 1 \equiv 1\,(8)$ and $7^2 \equiv (-1)^2 = 1\,(8)$ so the same holds for any even power. It follows that $1 \equiv 6^y + 1\,(8)$ that is that $2^3|2^y3^y$.

(e) We have $2^y3^y = 7^z - 5^z = \left(5^{x/2} + 7^{z/2}\right)\left(5^{x/2} - 7^{z/2}\right)$ since both x, z are even. The sum of the two numbers $A = 5^{x/2} + 7^{z/2}$ and $B = 5^{x/2} - 7^{z/2}$ is $2 \cdot 5^{x/2}$ which is not divisible by 3, so one of the factors must be divisible by 3^y. The other factor is then at most 2^y so we must have $A = 3^y2^r$ and $B = 2^s$ where $r + s = y$. A, B are both even $(x, z \geq 2)$ so $r, s \geq 1$ but since $4 \nmid A + B$ not both of r, s are at least 2. It follows that $r = 1$ or $s = 1$.

(f) $B = 2$ is impossible since reducing mod 6 this means $(-1)^{x/2} - 1 \equiv 2\,(6)$ that is $(-1)^{x/2} \equiv 3\,(6)$ whereas the powers of -1 are ± 1. $B = 2^{y-1}$ and $A = 2 \cdot 3^y$ is also impossible: reducing these mod 7 we find $5^{x/2} \equiv 2^{y-1} \equiv 2 \cdot 3^y\,(7)$ that is $2^y \equiv 4 \cdot 3^y\,(7)$. Multiplying by $2 \cdot 4^y$ this reads $2 \equiv 2 \cdot (2 \cdot 4)^y \equiv 2 \cdot 4 \cdot (3 \cdot 4)^y \equiv 5^y\,(7)$ so $y \equiv 4\,(6)$ and $8|B$, that is$5^{x/2} - 7^{z/2} \equiv 0\,(8)$. The powers of 5 mod 8 are $5, 1$ and of 7 are $7, 1$ so both $x/2$ and $z/2$ are even. Factoring again we have $\left(5^{x/4} + 7^{z/4}\right)\left(5^{x/4} - 7^{z/4}\right) = 2^{y-1}$. Again both factors cannot be divisible by 4, but now both are powers of 2 so $5^{x/4} - 7^{z/4} = 2$. We have already seen that this cna't happen (the case $B = 2$) so the equation has no solutions.