Elementary Number Theory

Midterm Review Exercises

A Selection of Exercises on Divisibility, Prime Numbers, Congruences, Congruences with a Prime-power Modulus, Euler's Function, Group of Units and Quadratic Residues

Andrew Dong

supervised by
Professor Ngo Bau Chau
special thanks to Minh-Tam Trinh

November 12, 2015

Problems on Divisibility

Divisors

Exercise 1.1

Exercise: Find a shorter proof for Example 1.2, based on putting b = 2 in Theorem 1.1
Solution:
Example 1.2 makes the claim that if n is a square then n leaves a remainder 0 or 1 when divided by 4.

Theorem 1.1 states that if a and b are integers with $b > 0$ then there is a unique pair of integers q and r such that

$$a = qb + r$$

and

$$0 \leq r < b$$

.

Letting a = 2q + r with r = 0 or 1, we get return the equation

$$n = a^2 = (2q + 4)^2 = 4(q^2 + qr) + r^2$$

with $r^2 = 0$ or 1. □

Bezout's Identity

Exercise 1.9

Exercise: Prove that $\gcd(a_1, ..., a_k) = \gcd(\gcd(a_1, a_2), a_3, ..., a_k)$.
Solution:
We know that an integer c divides $a_1, ..., a_k$ if and only if it divides $\gcd(a_1, a_2)$, $a_3, ..., a_k$. The largest c for which this is true is the greatest common divisor for both $a_1, ..., a_k$ and $\gcd(a_1, a_2)$, $a_3, ..., a_k$ by definition. Formalizing this statement we get that $\gcd(a_1, ..., a_k) = \gcd(\gcd(a_1, a_2), a_3, ..., a_k)$. □

Least Common Multiples

Exercise 1.14

Exercise: Show that c is a common multiple of a and b if and only if it is a multiple of l = lcm(a,b).
Solution:
By theorem 1.1 which is stated above, we have that c = ql + r. Since a and b both divide c and l, they divide r as well, which implies that r is a common multiple. However, since l is the least common multiple, r = 0 which implies that l divides c. □

Linear Diophantine Equations

Exercise 1.16

Exercise: If $a_1, ..., a_k$ and c are integers, when does the Diophantine equation $a_1x_1 + ... + a_kx_k = c$ have integer solutions $x_1, ..., x_k$?
Solution:

We know that the gcd$(a_1, ..., a_k) = a_1x_1 + ... + a_kx_k$ for some $x_k \in Z$. Thus the Diophantine equation $a_1x_1 + ... + a_kx_k = c$ has integer solutions $x_1, ..., x_k$ if and only if the gcd of $a_1, ..., a_k$ divides the integer c.

Supplementary Exercises on Divisibility

Exercise 1.18

Exercise: The Fibonacci numbers f_n = 1,1,2,3,5,... are defined by $f_1 = f_2 = 1$ and $f_{n+2} = f_{n+1} + f_n$ for all $n \geq 1$. Show that $0 \leq f_n < f_{n+1}$ for all $n \geq 2$. What happens if Euclid's algorithm is applied when a and b are a pair of consecutive Fibonacci numbers $f_{n+2} and f_{n+1}$? Show that $h(f_{n+2}) \geq n$.
Solution:
First let's understand that the height of an integer $a \geq 2$ is the greatest n such that Euclid's algorithm requires n steps to compute gcd(a,b) for some positive $b < a$, and it can be written as h(a).

Now, we consider an application of Euclid's algorithm. Since $0 \leq f_n < f_n + 1 \forall n \geq 2$, we know that $f_{n+2} = 1 * f_{n+1} + f_n$. We can continue inductively until gcd$(f_{n+2}, f_{n+1}) = f_2 = 1$. Since this takes n steps, we have that h$(f_{n+2}) \geq n$.

Problems on Prime Numbers

Prime numbers and prime-power factorisations

Exercise 2.4

Exercise: If m and n are positive integers, under what condition is $m^{1/n}$ rational?
Solution:
By a corollary we have that if a postive integer m is not a perfect square, them $\sqrt(m)$ is irrational. Thus, in order for $m^{1/n}$ to be rational we must have that m is the n-th power of an integer.

Distribution of Primes

Exercise 2.6

Exercise: Prove that every prime p $\neq$ 3 has the form 3q + 1 or 3q + 2 for some integer q; prove that there are infinitely many primes of the form 3q + 2.
Solution:
To show that every prime p $\neq$ 3 has the form 3q + 1 or 3q + 2, consider the equality p = 3q + x where x can equal 0, 1, or 2. If x = 0 then $3|p$, so p = 3 which contradicts hypothesis. Thus we conclude that x = 1 or 2. Now to prove that there are infinitely many, suppose on the contrary that there were only finitely many primes of the form $p_1, ..., p_k$. Let $m = 3p_1...p_k - 1$ so m also has the form 3q+3 with q = $p_1...p_k - 1$. Then since m is odd, so is each prime p dividing m so p has the form 3q + 1 or 3q + 3 for some q. If each p has the form 3q + 1, then m must also have this form which is false. This implies that m must be divisible by at least one prime of the form 3q + 3. But by assumption, p = p_i for some i, so p divides $3p_1...p_k - m = 1$ which is a contradiction. □

Fermat and Mersenne Primes

Exercise 2.10

Exercise: Prove Theorem 2.13.
If $m > 1$ and $a^m - 1$ is prime, then a = 2 and m is prime.
Solution:
Suppose a > 2. Then $a^m - 1 = (a-1)(a^{m-1} + a^{m-2} + ... + 1)$ is not prime. Therefore, we must have that a = 2. Now suppose m were not prime, that is suppose there exist r,s > 1 such that m = rs. Then $a^m - 1 = (a^r)^s - 1 = (a^r -)((a^r)^{s-1} + (a^r)^{s-2} + ... + 1)$ is also non-prime. Therefore, we must have that m is prime. Combining the two results above gives us our theorem. □

Primality-testing and Factorisation

Exercise 2.14

Exercise: Evaluate the Mersenne number $M_{13} = 2^{13} - 1$. Is it prime?
Solution:
Here we will use Lemma 2.14 which states that an integer is composite if and only if it is divisible by some prime less than or equal to the square root of the integer.
$M_{13} = 2^{13} - 1 = 8191$ is a prime number since no prime less than or equal to$\sqrt{8191} \sim 89$ is a divisor.

Supplementary Exercises on Primes

Exercise 2.18

Exercise: Show that if $p > 1$ and p divides (p-1)! + 1, then p is prime.
Solution:
Suppose p were not prime, ie. gcd(a,p)$\neq$1 for some a. Now consider such an a which divides p, which then also divides (p-1)! + 1 since p divides (p-1)! + 1. If a $<$ p then this implies that a is also a factor of (p-1)!. Notice then that a must be equal to 1, showing that the only integer which divides p is 1, meaning that p is a prime. □

Problems on Congruences

Modular Arithmetic

Exercise 3.3

Exercise: Find a proof of the fact that a(a+1)(2a+1) is divisible by 6 for every integer a, based on the observation that $6|m$ if and only if $2|m$ and $3|m$.
Solution:
Either a or a+1 must be even, thus 2 | a(a+1)(2a+1). If 3 | a or a+1 then 3 | a(a+1)(2a+1); if not then a ≡ 1 mod(3) which implies that 2a + 1 ≡ 3 ≡ 0 mod () and so $3|a(a+1)(2a+1)$. In both cases we observe that a(a+1)(2a+1) is divisible by 2 and 3, which implies that a(a+1)(2a+1) is divisible by 6. □

Linear Congruences

Exercise 3.6

Exercise: Show, by means of a counterexample, that Lemma 3.9(b) can fail if a and n are not coprime.

Lemma 3.9 states that if a and n are coprime and m divides a and b and $a\prime$ = a/m and $b\prime$ = b/m; then

$$ax \equiv bmod(n) \text{ if and only if } a\prime x \equiv b\prime mod(n).$$

Solution:
Consider the counterexample where a = 6 and b = 2 and m = 2. Then 6x ≡ 2 mod(4) has the solution of x ≡ $1or3$ but the congruence 3x ≡ 1 mod(4) has general solution x ≡ 3 mod (4). Contradiction.

Supplementary Exercises for Congruences

Exercise 3.18

Exercise: Seven thieves try to share a hoard of gold bars equally between themselves. Unfortunately, six bars are left over, and in the fight over them, one thief is killed. The remaining six thieves, still unable to share the bars equally since two are left over, again fight, and another is killed. When the remaining five share the bars, one bar is left over, and it is only after yet another thief is killed that an equal sharing is possible. What is the minimum number of bars which allows this to happen?
Solution:
This question can be modeled in terms of congruences. The first congruence, in which seven thieves must be matched to 6 bars can be written $x \equiv 6$ mod 7. The second congruence in which six thieves must fight over 2 bars can be written $x \equiv 2$ mod 6. The third congruence in which 5 thieves fight over 1 bar can be written $x \equiv 1$ mod 5. The final congruence can be written $x \equiv 0$ mod 4. The general solution for this can be written x ≡ 356 mod (420). Solving this congruence we get that the smallest solution is x = 356. This is the minimum number of bars which allows this an equal sharing to be possible.

Problems on Congruences with a Prime-power Modulus

The Arithmetic of Z_P

Exercise 4.3

Exercise: Prove Wolstenholme's Theorem. That is, prove that if p is an odd prime then the numerator of the rational number

$$r = 1 + 1/2 + 1/3 + ... + 1/p - 1$$

(in reduced form) is divisible by p; prove that if $p > 3$ then it is divisible by p^2.
Solution:
By simplifying r we have $r = (n_1 + ... + np - 1)/(p - 1)!$ where $n_i = (p - 1)!/i$ for each i. By corollary that an integer n is prime if and only if (n-1)! $\equiv$ -1 mod (n), we have that (p-1)! $\equiv$ -1 mod (p) which implies that p does not divide the denominator. p divides the numerator $n_1 + ... + n_{p-1}$ of r.

not sure how to properly finish this proof

Solving Congruences mod (p^e)

Exercise 4.14

Exercise: Show that $k_i \equiv 2$ mod (5) for all i in example 4.9.
Solution:
$q_{i+1} = (2x_{i+1} - 3_/5^{i+1} = (2(x_i + 2.5^i q_i) - 3)/5^{i+1} = ((2x_i - 3) + 4.5^i q_i)/5_{i+1} = (q_i + 4q_i)/5 = q_i$. Since $2x_1$ - 3 = 5 we have $q_i = 1$ for all i so $k_i \equiv 2$ as desired. □

Supplementary Exercises for Congruences with a Prime-power modulus

Exercise 4.17

Exercise: A function f from Z_p to Z_p is a polynomial function if there is a polynomial g(x), with integer coefficients, such that f(x) = g(x) in Z_p for all $x \in Z_p$. Two distinct polynomials can define the same function on Z_p: for instance, the polynomials x and x^p, by Corollary 4.4. Show that there are exactly p^p polynomial functions $Z_p \to Z_p$, and deduce that every function $Z_p \to Z_p$ is a polynomial function.
Solution:
Recall that $x^p = x$. Reducing coefficients mod(p), we can assume that $g(x) = \sum_{i=0}^{p-1} a_i x^i$ with $0 \leq a_i < p \forall i$. There are p^p polynomial functions since if two polynomials induce the function then their difference has p roots in Z_p which implies that the two polynomials are equal. Consider two finite sets A and B. There are $|B|^{|A|}$ functions $A \mapsto B$ since there are $|B|$ possible images of each which implies that there are p^p functions $Z_p \mapsto Z_p$, so each is polynomial.

Problems on Euler's Function

Units

Exercise 5.2

Exercise: Show that the group U_n is abelian.
Solution:
To be abelian we must have that [a][b] = [b][a] for all [a],[b]$\in Z_n$. Well, [a][b]=[ab] and [b][a]=[ba] since ab = ba for all a,b $\in Z$. Thus the desired result follows. □

Euler's Function

Exercise 5.8

Exercise: Show that for each integer m, there are only finitely many integers n such that $\phi(n) = m$
Solution:
$\forall p^e$ dividing n, $(p-1)p^{e-1}$ divides $\phi(n) = m$ which results in

$$p^e \leq mp/(p-1) \leq 2m$$

. There are only finitely many prime powers for which $p^e \leq 2m$ which implies that there are only finitely many integers n such that $\phi(n) = m$. □

Applications of Euler's Function

Exercise 5.19

Exercise: If my public key is the pair n = 10147, e = 119, then what is my decoding transformation?
Solution:
n = 10147 = 73 * 139 which implies that $\phi(n)$ = 72 * 138 = 9936. For e = 119, the inverse in $U_9$936 is f = 167 since 119*167 = 19873 = 2 * 9936 + 1 = e * f. Thus, we write our decoding transformation as

$$x \mapsto x^{167} mod(10147)$$

Problems on The Group of Units

The Group U_n

Exercise 6.2

Exercise: Show that if l and m are positive integers with highest common factor h, then $gcd(2^l - 1, 2^m - 1)$ divides $2^h - 1$.
Solution:
Let k be the order of the element 2 in the group U_n. Since h divides $2^l - 1$, $2^l = 1$ in U_n which implies that $k|l$. Similarly k divides m, so $k|gcd(l, m) = h$. Then $2^n = 1$ in U_n since $2^k = 1$ and $k|h$ which implies that $n|2^n - 1$. □

Primitive Roots

Exercise 6.5

Exercise: Show that if U_n has a primitive root then it has $\phi(\phi(n))$ of them.
Solution:
Suppose a is a primitive root of U_n. Then we know that U_n is cyclic and can be generated by a. The order of U_n can be written as $m = \phi(n)$. Thus, we see that U_n can be generated by a^k if and only if k and m are relatively prime. The number of primitive roots a^k is $\phi(m) = \phi(\phi(n))$. □

The group U_{p^e}, where p is an odd prime

Exercise 6.8

Exercise: Verify that 2 is a primitive root mod (25) by calculating its powers.
Solution:
To verify that 2 is a primitive root mod(25), we consider the powers of 2 in the unit group U_25. The powers of 2 are $\{2, 4, 8, 16, 7, 14, 3, 6, 12, 24 = -1, -2 = 23, -4 = 21, -8 = 17, -16 = 9, 18, 11, 22 = -3, -6 = 19, -12 = 13, 1\}$. Thus 2 has order $20 = \phi(25)$ which implies that 2 is a primitive root mod(25).

The group U_{2^e}

Exercise 6.11

Exercise: Find the order of each element of U_16.
Solution:
$U_{16} = \{1, 3, 5, 7, 9, 11, 13, 15\}$. 1 has order 1, 3 has order 4, 5 has order 4, 7 has order 2, 9 has order 2, 11 has order 4, 13 has order 4, and 15 has order 2

Applications of primitive roots

Exercise 6.15

Exercise: Solve the congruence $x^6 \equiv 4 \bmod (23)$
Solution:
We know that 5 is a primitive root mod (23) by a previous exercise, so we know that $4 \equiv 5^4 \bmod (23)$.

Letting $x = 5^i$ we get that $5^{6i} \equiv 5^4$ mod (23). This means that $6i \equiv 4$ mod (22), where $i \equiv 8, 19$ mod (22). Therefore we get that $x \equiv 5^8, 5^{19} \equiv \pm 7$ mod (23).

The Universal Exponent

Exercise 6.19

Exercise: Show that a finite abelian group G satisfies e(G) = $|G|$ if and only if G is cyclic. For which integers n is e(n) = $\phi(n)$?
Solution:
Suppose G is cyclic. Then it has an element of order $|G|$, and every element has order dividing $|G|$, so e(G) = $|G|$. If we let e(g) = $|G| = \prod p_i^{e_i}$ with each p_i prime, we have that G contains some g_i with order $p_i^{e_i}$ for each i. Since these orders commute and have coprime orders, we know that $\prod g_i$ has order $\prod p_i^{e_i}$, thereby generating G. This implies that e(n) = $\phi(n)$ if and only if U_n is cyclic. □

Supplementary Exercises on the group of units

Exercise 6.24

Exercise: For which Fermat primes and Mersenne primes is 2 a primitive root?
Solution:
If p = $F_n = 2^{e^n} + 1$ with $n \geq 2$, then 2 has order $2^{n+1} < 2^{2^n} = \phi(p)$ in U_p. Similarly, if p = $M_l = 2^l - 1$ with $p \geq 3$, then 2 has order $l < 2^l - 2 = \phi(p)$ in U_p. Thus, 2 is a primitive root only for $p = F_0 = M_2 = 3$ and $p = F_1 = 5$.

Problems on Quadratic Residues

Quadratic Congruences

Exercise 7.1

Exercise: Find all the solutions in Z_15 of the congruence $x^2 - 3x + 2 \equiv 0$ mod (15).
Solution:
Recall the formula

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a} \tag{1}$$

which can be rewritten

$$(2ax + b)^2 = b^2 - 4ac \tag{2}$$

Applying formula we get that x = 1,2,7,11 in Z_{15}

The group of quadratic residues

Exercise 7.3

Exercise: Find Q_n for each $n \leq 12$.
Solution:
$Q_1 = \{1\}$,
$Q_2 = \{1\}$,
$Q_3 = \{1\}$,
$Q_4 = \{1\}$,
$Q_5 = \{1, 4\}$,
$Q_6 = \{1\}$,
$Q_7 = \{1, 2, 4\}$,
$Q_8 = \{1\}$,
$Q_9 = \{1, 4, 7\}$,
$Q_{10} = \{1, 9\}$,
$Q_{11} = \{1, 3, 4, 5, 9\}$,
$Q_{12} = \{1\}$

The Legendre symbol

Exercise 7.8

Exercise: Determine whether 3 and 5 are quadratic residues mod (29).
Solution:
Consider $3^3 \equiv -2$, so $3^14equiv(-2)^4 * 3^2 \equiv 144 \equiv -1$ which implies that $3 \notin Q_{29}$.
Furthermore, consider $5^2 \equiv -4$, so $5^6 \equiv -64 \equiv -6$, which implies thta $5^{14} \equiv (-6)^2 * (-4) \equiv -144 \equiv 1$, giving us the result that $5 \in Q_{29}$. Thus, 5 is a quadratic residue mod(29) but 3 is not.

Quadratic Reciprocity

Exercise 7.11

Exercise: Is 219 a quadratic residue mod (383)?
Solution:
Notice that 383 is prime but 219 is not. In fact, 219 can be factorized to 219 = 3 * 73, implying that $(\frac{219}{383}) = (\frac{3}{383})(\frac{73}{383})$. By the quadratic reciprocity law (which I can now prove in 3 ways!), we have that $(\frac{3}{383}) = -(\frac{383}{3}) = -(\frac{2}{3}) = 1$ and similarly $(\frac{73}{383}) = (\frac{383}{73}) = (\frac{18}{73}) = (\frac{2}{73})(\frac{3}{73})^2 = (\frac{2}{73}) = 1$ which implies that $(\frac{219}{383}) = 1$ and thus 219 is indeed $\in Q_{383}$

Quadratic residues for prime-power moduli

Exercise 7.14

Exercise: Find the square roots of 6 mod (5^4).
Solution:
To find the square roots of 6 mod (5^4) we first notice that $16^2 = 6 + 5^3 * 2$. Solving for 2 + 32k ≡ 0 mod (5) gives k = -1 and$s = 16 + 5^3 * (-1)$, thus the square roots of 6 mod (5^4) are ± 109.

Supplemental Exercises on Quadratic Residues

Exercise 7.20

Exercise: Show that, for each $r \geq 1$, there are infinitely many primes $p \equiv 1$ mod (2^r).
Solution:
Supose there are instead finitely many primes $p \equiv 1$ mod (2^r). Name them $p_1, ..., p_k$ and define a = $2p_1 * ... * p_k$ and $m = a^{2^{2-1}} + 1$ which is divisible by an odd prime p. Since a has order 2^r in U_p, by Lagrange's theorem we have that $2^r | p - 1$. This implies the congruence $p \equiv 1 mod(2^r)$ which means that p = p_i for some i and p divides a. But since p divies m, we have that $p | m - a^{2r-1} = 1$, which is a contradiction. Thus, there must be infinitely many primes $p \equiv 1$ mod (2^r). $\square$