

## HOMEWORK FOR THE COURSE “NUMBER THEORY”

LECTURER: S.A. MERKULOV

### 1. CHAPTER 1

**Exercise 10.** Suppose that  $u, v \in \mathbb{Z}$  and  $(u, v) = 1$ . Show that  $(u + v, u - v)$  is either 1 or 2.

**Exercise 17.** Prove that  $\sqrt{2}$  is irrational, i.e., that there is no rational number  $r = a/b$  such that  $r^2 = 2$ .

**Exercise 25.** If  $a^n - 1$  is a prime, show that  $a$  is even and that  $n$  is a prime. (Primes of the form  $2^p - 1$  are called Mersenne primes)

**Exercise 28.** For all  $n$  show that  $30|n^5 - n$  and  $42|n^7 - n$ .

**Exercise 30.** Prove that  $\frac{1}{2} + \frac{1}{3} + \dots + \frac{1}{n}$  is not an integer.

### 2. CHAPTER 2

**Exercise 6.** For a rational number  $r$  let  $[r]$  be the largest integer less than or equal to  $r$ . Prove  $\text{ord}_p n! = [n/p] + [n/p^2] + [n/p^3] + \dots$

**Exercise 15.** Show that

- (a)  $\sum_{d|n} \mu(n/d)\nu(d) = 1$  for all  $n$ .
- (b)  $\sum_{d|n} \mu(n/d)\sigma(d) = n$  for all  $n$ .

**Exercise 17.** Show that  $\sigma(n)$  is odd iff  $n$  is a square or twice a square.

### 3. CHAPTER 3

**Exercise 5.** Show that the equation  $7x^3 + 2 = y^3$  has no solution in integers.

**Exercise 12.** Let  $\binom{p}{k} = \frac{p!}{k!(p-k)!}$  be a binomial coefficient, and suppose that  $p$  is a prime. If  $1 \leq k \leq p - 1$ , show that  $p$  divides  $\binom{p}{k}$ . Deduce  $(a + 1)^p \equiv a^p + 1 \pmod{p}$ .

**Exercise 13.** Use Exercise 12 to give another (than in the lecture/book) proof of Fermat's theorem,  $a^{p-1} \equiv 1 \pmod{p}$  if  $p \nmid a$ .

**Exercise 16.** Use the proof of the Chinese Remainder Theorem to solve the system  $x \equiv 1 \pmod{7}$ ,  $x \equiv 4 \pmod{9}$ ,  $x \equiv 3 \pmod{5}$ .

### 4. CHAPTER 4

**Exercise 6.** If  $p = 2^n + 1$  is a Fermat prime, show that 3 is a primitive root modulo  $p$ .

**Exercise 18.** Solve the congruence  $1 + x + x^2 + \dots + x^6 \equiv 0 \pmod{29}$ .

**Exercise 22.** If  $a$  has order 3 modulo  $p$ , show that  $1 + a$  has order 6.

## 5. CHAPTER 5

**Exercise 4.** Prove that  $\sum_{a=1}^{p-1} (a/p) = 0$ .

**Exercise 6.** Show that the number of solutions to  $x^2 - y^2 \equiv a \pmod{p}$  is given by

$$\sum_{y=0}^{p-1} (1 + ((y^2 + a)/p)).$$

**Exercise 11.** Suppose that  $p = 3$  (4) and that  $q \equiv 2p + 1$  is also prime. Prove that  $2^p - 1$  is not prime. (*Hint:* Use the quadratic character of 2 to show that  $q|2^p - 1$ .) One must assume that  $p > 3$ .

**Exercise 13.** Show that any prime divisor of  $x^4 - x^2 + 1$  is congruent to 1 modulo 12.

**Exercise 16.** Using the quadratic reciprocity find the primes for which 7 is a quadratic residue.

## 6. CHAPTER 6

**Exercise 1.** Show that  $\sqrt{2} + \sqrt{3}$  is an algebraic integer.

**Exercise 10.** What is  $\sum_{a=1}^{p-1} g_a$ .

**Exercise 18.** Show that there exist algebraic numbers of arbitrary high degree.

## 7. CHAPTER 7

**Exercise 3.** Let  $F$  be a field with  $q$  elements and suppose that  $q \equiv 1 \pmod{n}$ . Show that for  $\alpha \in F^*$  the equation  $x^n = \alpha$  has either no solutions or  $n$  solutions.

**Exercise 4** (Continuation). Let  $K$  be a field containing  $F$  such that  $[K : F] = n$ . For all  $\alpha \in F^*$  show that the equation  $x^n = \alpha$  has  $n$  solutions in  $K$ . [*Hint:* Show that  $q^n - 1$  is divisible by  $n(q - 1)$  and use the fact that  $\alpha^{q-1} = 1$ .]

**Exercise 6.** Let  $K \supset F$  be finite fields with  $[K : F] = 3$ . Show that if  $\alpha \in F$  is not a square in  $F$ , it is not a square in  $K$ .

## 8. CHAPTER 9

**Exercise 1.** If  $\alpha \in \mathbb{Z}[\omega]$ , show that  $\alpha$  is congruent to either 0, 1 or  $-1$  modulo  $1 - \omega$ .

## 9. CHAPTER 10

**Exercise 4.** The hypersurface defined by a homogeneous polynomial of degree 1,  $a_0x_0 + a_1x_1 + \dots + a_nx_n$ , is called a hyperplane. Show that any hyperplane in  $P^n(F)$  has the same number of elements as  $P^{n-1}(F)$ .

## 10. CHAPTER 12

**Exercise 3.** Describe the units in  $\mathbb{Q}(\sqrt{5})$ .

**Exercise 7.** Show that the class number of  $\mathbb{Q}(\sqrt{5})$  is greater than one.

**Exercise 18.** (Theorem on a primitive element.) If  $F$  is an algebraic number field show that there exists an element  $\gamma \in F$  such that  $\mathbb{Q}(\gamma) = F$ .

## 11. CHAPTER 13

**Exercise 2.** Let  $F$  be a real quadratic field. Show that if  $F$  has an element of norm  $-1$  then no prime  $p \equiv 3 \pmod{4}$ .

**Exercise 8.** Show that the class number of  $\mathbb{Q}(\sqrt{10})$  is not 1.

## 12. CHAPTER 17

**Exercise 2.** Find the integral solutions to  $y^2 + 31 = x^3$ .

SERGEI A. MERKULOV: DEPARTMENT OF MATHEMATICS, STOCKHOLM UNIVERSITY, 10691 STOCKHOLM, SWEDEN  
*E-mail address:* `sm@math.su.se`