

# Questions for the exam

October 18, 2009

## 1 Theoretical questions

1. Formulate binomial theorem. Right the formula for  $(x+y)^n$  and formula for the binomial coefficients.
2. For two positive integer numbers  $n, m$  define  $gcd(n, m)$  and prove that it exists. You can not use prime number factorization, you can use well ordering principle.
3. For two polynomials  $n(x), m(x)$  define  $gcd(n(x), m(x))$  and prove that it exists.
4. Prove that if integers numbers  $a$  and  $c$  are relatively prime and  $c$  divides  $ab$  then  $c$  divides  $b$ .
5. Prove that if polynomials  $a(x)$  and  $c(x)$  are relatively prime and  $c(x)$  divides  $a(x)b(x)$  then  $c(x)$  divides  $b(x)$ .
6. Prove that there are infinitely many prime numbers.
7. Prove that if a product of several numbers is divisible by a prime number  $p$  then one of them is divisible by  $p$ .
8. Prove that if a product of several polynomials is divisible by an irreducible polynomial  $p(x)$  then one of them is divisible by  $p(x)$ .
9. a) Prove that any positive integer number could be written as a product of prime numbers

$$n = p_1 p_2 \cdots p_k$$

- b) Prove that the factorization is unique in the sense that if also

$$n = q_1 q_2 \cdots q_l$$

then  $l = k$  and we can renumber the  $q_i$ , so that  $q_i = p_i$ .

10. Prove that any polynomial with rational coefficients could be written as a product of irreducible over  $\mathbb{Q}$  polynomials.
11. What polynomials are irreducible over  $\mathbb{C}$ ? What polynomials are irreducible over  $\mathbb{R}$ ? You don't need to prove it, only describe them so it was easy to check if polynomial is irreducible or not.
12. Prove that  $\sqrt{2}, \sqrt{6}$  are irrational.
13. Prove that  $\sqrt{x^2 + x + 1}$  can not be written as a ratio of two polynomials with real coefficients.

## 2 Skills

14. Prove using mathematical induction

- a) Formulas.
- b) Inequalities.
- c) Divisibility.
- d) Everything else.

15. Write down binomial formula for a particular  $n$ . Recognize binomial formula.

16. For two integer numbers  $a, b$  find  $\gcd(a, b)$ . Write down it in the form

$$d = an + bm$$

17. For two polynomials  $a(x), b(x)$  find  $\gcd(a, b)$ . Write down it in the form

$$d = a(x)n(x) + b(x)m(x)$$

18. If  $a, b$  and  $c$  are integer numbers find if the equation

$$ax + by = c$$

has a solution in integer numbers. If it does find one at least one solution.

19. If  $a(x), b(x)$  and  $c(x)$  are polynomials find if there exist polynomials  $p(x)$  and  $q(x)$  such that

$$a(x)p(x) + b(x)q(x) = c(x)$$

If they exist find at least one solution.

20. What is the definition of invertible element in  $\mathbb{Z}_n$ ? When  $a$  is invertible in  $\mathbb{Z}_n$ ? Find  $a^{-1} \pmod n$  if it exists.

21. Define what numbers are divisors of zero in  $\mathbb{Z}_n$ . When  $a$  is divisor in  $\mathbb{Z}_n$ ?

22. Solve the equation  $ax = b \pmod n$ . How many solutions it has?

23. Simplify  $\overline{a_n \cdots a_1 a_0}$  by module  $m$ .

24. Find if a polynomial is irreducible over  $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ .

25. Factor out a polynomial in irreducible factors over  $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ .

26. All problems from homework 1-7 (Except problems 5 in homework 1,3,4,6,7)

### 3 Sample Exam

**Problem 1.** Prove by induction that if  $a > -1$  and  $n > 1$  then  $(1+a)^n > 1+na$ .

**Problem 2.** Prove that there is only one way to write a number  $n$  as a product of prime numbers

$$n = p_1 p_2 \cdots p_k$$

in the sense that if

$$n = q_1 q_2 \cdots q_l$$

then  $l = k$  and we can renumber the  $q_i$ , so that  $q_i = p_i$ .

**Problem 3.** Find at least one solution of

$$(x^3 + x^2 + x + 1)n(x) + (x^3 + x^2)m(x) = x^2 + 3x + 2$$

**Problem 4.** Prove that  $\overline{a_4 a_3 a_2 a_1 a_0} \equiv a_4 + a_2 + a_0 - (a_3 + a_1) \pmod{11}$ .

**Problem 5.** List all numbers in  $\mathbb{Z}_{20}$  which are invertible.

**Problem 6.** Solve the following equation:

$$74x = 111 \pmod{407}$$

**Problem 7.** Find irreducible factor decomposition of  $x^3 + x^2 + x + 1$  over  $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ .