

## MIDTERM EXAM

Only a single hand-written “crib” sheet can be used, no books or notes. Even if I ask for just a yes/no answer, you must always give a proof. You may get some points even if you write “I don’t know”, but if you write something that is wrong, you may get less. (It is not possible to pass just writing “I don’t know” everywhere. . . .)

Solve 4 of the following problems. If you solve more, your 4 best solutions will be chosen.

**Problem 1.** (15) Show, via rough estimates, that the infinite series  $\frac{1}{2 \cdot 3} + \frac{1}{4 \cdot 5} + \frac{1}{6 \cdot 7} + \dots$  has a finite sum. [Hint: recall the method used for the sum  $1 + 1/2 + 1/3 + \dots$ .]

*Solution.* The series can be written as  $\sum_{i=1}^{\infty} \frac{1}{2i(2i+1)}$ . As in the method of the hint, let us group the terms between  $i = 1, 2, 4, 8, \dots$ . Thus, one group consists of all  $2^k \leq i < 2^{k+1}$ . The number of terms in this sum is  $2^k$ , and each term is of size  $\leq \frac{1}{2^{k+1}(2^{k+1}+1)} < 2^{-2(k+1)}$ . Therefore the total is at most  $2^k$  times this much, which is  $2^{-k-2}$ . Therefore the original sum can be estimated by  $\sum_{k=1}^{\infty} 2^{-k-2}$ , which as a decreasing geometric series, is known to have a finite sum.

**Problem 2.** (15) Find positive integers  $a, b, c$  such that  $\gcd(a, b) > 1$ ,  $\gcd(b, c) > 1$  and  $\gcd(a, c) > 1$  but  $\gcd(a, b, c) = 1$ . Compute  $\text{lcm}(a, b, c)$  (explaining the result).

*Solution.* Let  $a = 2 \cdot 3 = 6$ ,  $b = 3 \cdot 5 = 15$ ,  $c = 2 \cdot 5 = 10$ . Then  $\gcd(a, b) = 3$ ,  $\gcd(b, c) = 4$ ,  $\gcd(a, c) = 2$ . But there is no prime number dividing all three of  $a, b, c$ , therefore  $\gcd(a, b, c) = 1$ . We have  $\text{lcm}(a, b, c) = 2 \cdot 3 \cdot 5$ , this is the number containing each prime divisor of  $a, b, c$  with the largest exponent that occurs in them.

**Problem 3.** Estimate the number of computation steps that it takes to compute the number  $3^x$  for integer  $x$  (ordinary operations, not modulo anything) as a function of  $\text{len}(x)$ :

(a) (7) without repeated squaring,

*Solution.* There will be  $x$  multiplications. Each largest multiplication involves 3 and a number whose length is at most  $\text{len}(3^{x-1}) = O(x)$ . Such a multiplication takes  $O(x)$  steps. Therefore the number of steps is  $O(x \cdot x) = O(x^2) = O(2^{2\text{len}(x)})$ .

(b) (8) with repeated squaring.

*Solution.* The repeated squaring consists of  $O(\text{len}(x))$  multiplication operations. The length of the numbers can double at each squaring, so after the  $i$ th squaring is  $O(2^i)$ , and after the last squaring it is  $O(2^{\text{len}(x)}) = O(x)$ . The last term is Each squaring of a number of length  $k$  costs  $O(k^2)$  steps, so the number of steps is at the  $i$ th squaring is  $O(2^{2i})$ . The total number of steps is a geometric series whose last term of which is  $O(2^{2\text{len}(x)}) = O(x^2) = O(2^{2\text{len}(x)})$ , the same rate of growth as without repeated squaring.

**Problem 4.** (15) Find an integer  $z$  with the property that  $z \equiv 1 \pmod{230}$  and  $z \equiv -1 \pmod{81}$ . Show your work in a form followable for the grader.

*Solution.* Let us compute  $\gcd(230, 81)$  via the extended Euclidean algorithm.

$$\begin{array}{llll} r_0 = 230, & & s_0 = 1, & t_0 = 0, \\ r_1 = 81, & & s_1 = 0, & t_1 = 1, \\ q_1 = 2, & r_2 = r_0 - q_1 r_1 = 68, & s_2 = s_0 - q_1 s_1 = 1, & t_2 = t_0 - q_1 t_1 = -2, \\ q_2 = 1, & r_3 = r_1 - q_2 r_2 = 13, & s_3 = s_1 - q_2 s_2 = -1, & t_3 = t_1 - q_2 t_2 = 3, \\ q_3 = 5, & r_4 = r_2 - q_3 r_3 = 3, & s_4 = s_2 - q_3 s_3 = 6, & t_4 = t_2 - q_3 t_3 = -17, \\ q_4 = 4, & r_5 = r_3 - q_4 r_4 = 1, & s_5 = s_3 - q_4 s_4 = -25, & t_5 = t_3 - q_4 t_4 = 71, \end{array}$$

Hence  $\gcd(230, 81) = 1 = -25 \cdot 230 + 71 \cdot 81$ . It follows that  $-25 \cdot 230 \equiv 1 \pmod{81}$  and  $71 \cdot 81 \equiv 1 \pmod{230}$ . Therefore  $z = 71 \cdot 81 + 25 \cdot 230$  has the required properties.

**Problem 5.**

- (a) (8) Show that if  $\gcd(m, n) > 1$  then the set of equations  $x \equiv 1 \pmod{m}$ ,  $x \equiv 0 \pmod{n}$  is not solvable.

*Solution.* Let  $d = \gcd(m, n)$ ,  $m = m'd$ . If  $x \equiv 0 \pmod{n}$  then  $n|x$  and therefore  $d|x$ . But if  $x \equiv 1 \pmod{m}$  then  $x = 1 + km = 1 + km'd$  for some  $k$ , which shows that  $d$  does not divide  $x$ , a contradiction.

- (b) (7) Show that if  $\gcd(a, m) > 1$  then the equation  $a^x \equiv 1 \pmod{m}$  is not solvable.

*Solution.* Let  $d = \gcd(a, m)$ ,  $a = da'$ ,  $m = dm'$ . Then  $a^x = (da')^x$  is divisible by  $d$ . But if  $a^x \equiv 1 \pmod{m}$  then  $a^x = 1 + km = 1 + kdm'$  for some  $k$ , showing that  $a^x$  is not divisible by  $d$ . This contradiction shows that  $a^x \equiv 1 \pmod{m}$  is not solvable.

**Problem 6.** Consider the set  $M$  of all matrices of the form  $C(a, b) = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$  for  $a, b \in \mathbb{Q}$ .

- (a) (10) Show that  $M$  is a commutative ring with unity, under the usual matrix operations.

*Solution.* First we show that the sum and product of two matrices of this form is again of this form. For the sum, we have  $\begin{pmatrix} a & -b \\ b & a \end{pmatrix} + \begin{pmatrix} a' & -b' \\ b' & a' \end{pmatrix} = C(a + a', b + b')$ . For the product,

$$\begin{pmatrix} a & -b \\ b & a \end{pmatrix} \cdot \begin{pmatrix} a' & -b' \\ b' & a' \end{pmatrix} = \begin{pmatrix} aa' + (-b)b' & a(-b') + (-b)a' \\ ba' + ab' & b(-b') + aa' \end{pmatrix} = C(aa' - bb', ab' + ba').$$

The fact that the ring properties are satisfied follows from the fact that as shown in class, matrices form a ring with respect to matrix operations. The fact that the ring is commutative can be seen from  $C(aa' - bb', ab' + ba') = C(a'a - b'b, b'a + a'b)$ . It is also easy to see from this formula that  $C(1, 0)$  is a unity.

- (b) (5) Show that  $M$  is a field (elements other than 0 form a group under multiplication). [Hint: compute  $C(a, b) \cdot C(a, -b)$ .]

*Solution.* We have by the above formula  $C(a, b) \cdot C(a, -b) = C(a^2 + b^2, 0)$ . It follows that  $C\left(\frac{a}{a^2 + b^2}, \frac{-b}{a^2 + b^2}\right)$  is the inverse of  $C(a, b)$ .