

Number theory, Talteori 6hp, Kurskod TATA54, Provkod TEN1  
March 13, 2017  
LINKÖPINGS UNIVERSITET  
Matematiska Institutionen  
Examinator: Jan Snellman

Each problem is worth 3 points. To receive full points, a solution needs to be complete. Indicate which theorems from the textbook that you have used, and include all auxiliary calculations.

No aids, no calculators, tables, nor textbooks.

1) Find all odd positive integers  $n$  such that  $n + 1$  is divisible by 3 and  $n + 2$  is divisible by 5.

2) Show that the congruence

$$x^3 + x + 1 \equiv 0 \pmod{11^n}$$

has a unique solution for every positive integer  $n$ .

3) The number 431 is a prime. Determine if the congruence

$$2x^2 - 6x + 38 \equiv 0 \pmod{431}$$

has any solutions.

4) How many primitive roots are there mod 5? Find them all. How many primitive roots are there mod 25? For each primitive root  $a$  mod 5 that you find, check which of the “lifts”

$$a + 5t, \quad 0 \leq t \leq 4$$

are primitive roots mod 25.

5) Determine the (periodic) continued fraction expansion of  $\sqrt{7}$ . Determine the solution  $(x, y) \in \mathbf{Z}^2$ ,  $x, y > 0$ , to  $x^2 - 7y^2 = 1$  with smallest  $x$ .

6) For each positive integer  $n$ , let  $g(n)$  denote the number of triples  $(a, b, c)$  of positive integers such that  $abc = n$ . Calculate  $g(p^e)$ , with  $p$  a prime, then show that  $g$  is a multiplicative arithmetic function and use this to give a formula for  $g(n)$  in terms of the prime factorisation of  $n$ .

(Hint: the number-of-divisors function  $\tau$  is the Dirichlet square of the constant-one function. What is the Dirichlet cube?).

Number theory, Talteori 6hp, Kurskod TATA54, Provkod TEN1  
March 13, 2017  
LINKÖPINGS UNIVERSITET  
Matematiska Institutionen  
Examinator: Jan Snellman

Solutions

- 1) Find all odd positive integers  $n$  such that  $n + 1$  is divisible by 3 and  $n + 2$  is divisible by 5.

**Solution:** The integer  $n$  is a solution to

$$\begin{aligned}n &\equiv 1 \pmod{2} \\n &\equiv -1 \pmod{3} \\n &\equiv -2 \pmod{5}\end{aligned}$$

So

$$n = 1 + 2t \equiv -1 \pmod{3} \quad \implies \quad t \equiv -1 \pmod{3},$$

hence

$$n = 1 + 2(-1 + 3s) = -1 + 6s.$$

Then

$$-1 + 6s \equiv -2 \pmod{5} \quad \implies \quad s \equiv -1 \pmod{5}$$

hence

$$n = -1 + 6(-1 + 5r) = -7 + 30r = 23 + 30r'.$$

Thus all positive integer solutions are  $n = 23 + 30r'$  with  $r' \geq 0$ .

- 2) Show that the congruence

$$x^3 + x + 1 \equiv 0 \pmod{11^n}$$

has a unique solution for every positive integer  $n$ .

**Solution:** Put  $f(x) = x^3 + x + 1$ , then  $f'(x) = 3x^2 + 1$ . By inspection, we see that  $x = r = 2$  is the unique solution mod 11. Furthermore,  $f'(r) = 3 * 2^2 + 1 = 13 \not\equiv 0 \pmod{11}$ , so this solution lifts to a solution mod  $11^n$  for all positive  $n$ .

3) The number 431 is a prime. Determine if the congruence

$$2x^2 - 6x + 38 \equiv 0 \pmod{431}$$

has any solutions.

**Solution:** There is a misprint in the problem, which makes it harder. I had intended to use

$$\begin{aligned} 2x^2 - 12x + 38 &\equiv 2(x^2 - 6x + 19) \equiv 2((x - 3)^2 - 9 + 19) \\ &\equiv 2((x - 3)^2 + 10) \pmod{431} \end{aligned}$$

Then the congruence is solvable if and only if -10 is a square mod 431. We have that

$$\left(\frac{-10}{431}\right) = \left(\frac{-1}{431}\right) \left(\frac{2}{431}\right) \left(\frac{5}{431}\right)$$

Here  $\left(\frac{-1}{431}\right) = -1$  since  $431 \equiv -1 \pmod{4}$ ,  $\left(\frac{2}{431}\right) = 1$  since  $431 \equiv -1 \pmod{8}$ , and finally,

$$\left(\frac{5}{431}\right) = \left(\frac{431}{5}\right) = \left(\frac{1}{5}\right) = 1$$

by quadratic reciprocity (since  $5 \equiv 1 \pmod{4}$ ) and since  $431 \equiv 1 \pmod{5}$ . It follows that  $\left(\frac{-10}{431}\right) = -1 * 1 * 1 = -1$ , so -10 is not a square mod 431, and the congruence has no solution.

However, the actual congruence is  $2x^2 - 6x + 38$ , which makes the calculations messier.

$$\begin{aligned} 2x^2 - 6x + 38 &\equiv 2(x^2 - 3x + 19) \equiv 2\left(\left(x - \frac{3}{2}\right)^2 - \frac{9}{4} + 19\right) \\ &\equiv 2\left(\left(x + 214\right)^2 + 91\right) \pmod{431} \end{aligned}$$

since  $1/4 \equiv 108 \pmod{431}$  and  $1/2 \equiv 216 \pmod{431}$ . We now need to check if 91 is a square mod 431.

Since  $431 \equiv 3 \pmod{4}$  we have that

$$\left(\frac{91}{431}\right) = \left(\frac{7}{431}\right) \left(\frac{13}{431}\right) = \left(-\left(\frac{431}{7}\right)\right) \left(\frac{431}{13}\right) = -\left(\frac{4}{7}\right) \left(\frac{2}{13}\right) = -1 * (-1) = 1,$$

so this congruence does have solutions. In fact, since  $x = 214 \pm y \pmod{431}$ , where  $y^2 \equiv 91 \pmod{431}$ , which means that  $y \equiv \pm 130 \pmod{431}$ , the solutions to the congruence are  $x \equiv 87 \pmod{431}$  and  $x \equiv 347 \pmod{431}$ .

- 4) How many primitive roots are there mod 5? Find them all. How many primitive roots are there mod 25? For each primitive root  $a$  mod 5 that you find, check which of the “lifts”

$$a + 5t, \quad 0 \leq t \leq 4$$

are primitive roots mod 25.

**Solution:** There are  $\phi(\phi(5)) = \phi(5-1) = \phi(4) = 4-2 = 2$  primitive roots modulo 5. Obviously 1 and -1 are not primitive roots, so the primitive roots are 2 and 3.

There are  $\phi(\phi(25)) = \phi(25-5) = \phi(20) = \phi(4*5) = \phi(4)*\phi(5) = 2*4 = 8$  primitive roots mod 25. Furthermore,  $\mathbf{Z}_{25}^x$  has  $\phi(25) = 20$  elements, so an element of  $\mathbf{Z}_{25}^x$  has order a divisor of 20, and is a primitive root iff it has order 20.

We first check the lifts of 2,

$$x = 2 + 5t, \quad 0 \leq t \leq 4.$$

We see that  $7^2 = 49 \equiv -1 \pmod{25}$ , so  $7^4 \equiv 1 \pmod{25}$ , but the other lifts have all order 20, and are primitive roots.

Similarly, for the lifts of 3,  $18^2 \equiv (-7)^2 \equiv 49 \equiv -1 \pmod{25}$ , so  $18^4 \equiv 1$ . The other lifts have all order 20, and are primitive roots.

- 5) Determine the (periodic) continued fraction expansion of  $\sqrt{7}$ . Determine the solution  $(x, y) \in \mathbf{Z}^2$ ,  $x, y > 0$ , to  $x^2 - 7y^2 = 1$  with smallest  $x$ .

**Solution:** Put  $\alpha = \alpha_0 = \sqrt{7}$ . Then  $a_0 = \lfloor \alpha_0 \rfloor = 2$ ,

$$\alpha_1 = \frac{1}{\alpha_0 - a_0} = \frac{1}{\sqrt{7} - 2} = \frac{\sqrt{7} + 2}{3} = 1 + \frac{\sqrt{7} - 1}{3},$$

so  $a_1 = \lfloor \alpha_1 \rfloor = 1$ . Continuing, we get that  $a_2 = a_3 = 1$ ,  $a_4 = 4$ , and that  $\alpha_5 = \alpha_1$ . Hence, the periodic expansion is

$$\sqrt{7} = [2, \overline{1, 1, 1, 4}].$$

The convergents  $C_k = p_k/q_k$  are obtained from the recurrence

$$\begin{aligned} p_{k+1} &= a_{k+1}p_k + p_{k-1} \\ q_{k+1} &= a_{k+1}q_k + q_{k-1} \end{aligned}$$

with initial values  $q_{-2} = 1, p_{-2} = 0, q_{-1} = 0, p_{-1} = 1$ . This gives

$$C_0 = 2, C_1 = 3, C_2 = 5/2, C_3 = 8/3.$$

We have that  $8^2 - 7 * 3^2 = 1$ , and  $(x, y) = (8, 3)$  is the fundamental solution to Pell's equation.

- 6) For each positive integer  $n$ , let  $g(n)$  denote the number of triples  $(a, b, c)$  of positive integers such that  $abc = n$ . Calculate  $g(p^e)$ , with  $p$  a prime, then show that  $g$  is a multiplicative arithmetic function and use this to give a formula for  $g(n)$  in terms of the prime factorisation of  $n$ .

(Hint: the number-of-divisors function  $\tau$  is the Dirichlet square of the constant-one function. What is the Dirichlet cube?).

**Solution:** Denote by  $\mathbf{1}$  the multiplicative arithmetic function which has constant value 1. Then

$$(\mathbf{1} * \mathbf{1})(n) = \sum_{d|n} \mathbf{1}(d)\mathbf{1}(n/d) = \sum_{n=ab} \mathbf{1}(a)\mathbf{1}(b) = \sum_{n=ab} 1.$$

where the last two sums are over all factorisations  $n = ab, a, b \in \mathbf{Z}, a, b > 0$ . Similarly,

$$\begin{aligned} (\mathbf{1} * \mathbf{1} * \mathbf{1})(n) &= \sum_{d|n} \mathbf{1}(d)(\mathbf{1} * \mathbf{1})(n/d) = \sum_{n=aB} \mathbf{1}(a)(\mathbf{1} * \mathbf{1})(B) \\ &= \sum_{n=aB} \mathbf{1}(a) \sum_{bc=B} \mathbf{1}(b)\mathbf{1}(c) = \sum_{n=abc} \mathbf{1}(a)\mathbf{1}(b)\mathbf{1}(c) = \sum_{n=abc} 1 = g(n). \end{aligned}$$

Since  $g$  is the iterated Dirichlet convolution of multiplicative functions, it follows that  $g$  is multiplicative. However,  $\mathbf{1} * \mathbf{1} = \tau$ , so

$$g(n) = (\mathbf{1} * \mathbf{1} * \mathbf{1})(n) = \mathbf{1} * (\mathbf{1} * \mathbf{1})(n) = (\mathbf{1} * \tau)(n) = \sum_{d|n} \tau(d).$$

We now let  $p$  be a prime,  $e$  a positive integer, and calculate

$$g(p^e) = \sum_{d|p^e} \tau(d) = \sum_{\ell=0}^e \tau(p^\ell) = \sum_{\ell=0}^e (\ell + 1) = (e + 2)(e + 1)/2.$$

Since  $g$  is multiplicative, we now conclude that

$$g\left(\prod_{j=1}^r p_j^{e_j}\right) = \prod_{j=1}^r \frac{(e_j + 2)(e_j + 1)}{2} = 2^{-r} \prod_{j=1}^r (e_j + 2)(e_j + 1).$$