Number theory, Talteori 6hp, Kurskod TATA54, Provkod TEN1
June 08, 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 auxillary calculations.

No aids, no calculators, tables, nor texbooks.

1) Use the Chinese Remainder Theorem to find all solutions to

$$x^2 \equiv 15 \mod 77.$$

2) For which positive n does the congruence

$$x^5 + x + 1 \equiv 0 \mod 5^n$$

have a unique solution? Find all solutions for $n = 1, 2$.

3) Let $x = [13; \overline{1, 7}]$. Compute the value of x.

4) The function f satisfies

$$\begin{aligned} f(1) &= 1 \\ f(1) + f(2) &= a \\ f(1) + f(3) &= b \\ f(1) + f(2) + f(4) &= c \\ f(1) + f(2) + f(3) + f(6) &= ab \\ f(1) + f(2) + f(3) + f(4) + f(6) + f(12) &= bc \end{aligned}$$

Calculate $f(12)$. For which a, b, c can f be extended to a multiplicative function on the positive integers?

5) Show that 10 is a primitive root modulo 17. List all quadratic residues mod 17.

6) The number 41 is a prime. Show that -1 is a quadratic residue module 41, then find a solution to the congruence

$$x^2 \equiv -1 \mod 41$$

Among the solutions (m, n) to

$$mx + n \equiv 0 \mod 41$$

find a pair with $0 < |m|, |n| \leq 6$. Show that $41 = m^2 + n^2$.

Number theory, Talteori 6hp, Kurskod TATA54, Provkod TEN1
June 08, 2017
LINKÖPINGS UNIVERSITET
Matematiska Institutionen
Examinator: Jan Snellman

Solutions

1) Use the Chinese Remainder Theorem to find all solutions to

$$x^2 \equiv 15 \mod 77.$$

Solution: Since $77 = 7 * 11$, we solve the congruence mod 7 and mod 11, then combine these solutions using the CRT.

$$x^2 \equiv 15 \equiv 1 \mod 7$$

has the solutions $x \equiv \pm 1 \mod 7$, and

$$x^2 \equiv 15 \equiv 4 \mod 11$$

has the solutions $x \equiv \pm 2 \mod 11$.

The Euclidean algorithm gives that

$$1 = \gcd(7, 11) = (-3) * 7 + 2 * 11$$

so

$$\begin{aligned} x &\equiv 1 \mod 7 \\ x &\equiv 2 \mod 11 \end{aligned}$$

gives

$$x = 7n + 1 = 11m + 2 \implies 7n - 11m = 1$$

which have the solutions

$$\begin{aligned} n &= -3 + 11s \\ m &= -2 + 7s \end{aligned}$$

hence $x = -20 + 77s$, so $x \equiv -20 \equiv 57 \mod 77$. The other combinations of solutions mod 7 and mod 11 lift to $x \equiv 13 \mod 77$, $x \equiv 20 \mod 77$, and $x \equiv 64 \mod 77$.

2) For which positive n does the congruence

$$x^5 + x + 1 \equiv 0 \mod 5^n$$

have a unique solution? Find all solutions for $n = 1, 2$.

Solution: Let $f(x) = x^5 + x + 1$. Then, by inspection, the congruence

$$f(x) \equiv 0 \mod 5$$

has the unique solution $x = 2$. Since $f'(x) = 5x^4 + 1$, we have that $f'(x) \equiv 1 \mod 5$, hence the zero mod 5 lifts uniquely to a zero mod 5^n for all n, by Hensel's lemma. For $n = 2$ we put

$s = 2 + 5t$ and calculate that

$$\begin{aligned}
0 &\equiv f(s) = f(2+5t) \mod 25 \\
&\equiv (2+5t)^5 + 5t + 3 \mod 25 \\
&\equiv (2^5 + \binom{5}{1}2^4(5t) + \binom{5}{2}2^3(5t)^2 + \binom{5}{3}2^2(5t)^3 + \binom{5}{4}2^1(5t)^4 + (5t)^5) + 5t + 3 \mod 25 \\
&\equiv 32 + 5t + 3 \mod 25 \\
&\equiv 10 + 5t \mod 25
\end{aligned}$$

so $t \equiv -2 \mod 25$ and the unique zero is $s = 2 + 5 * (-2) = -8 \equiv 17 \mod 25$.

3) Let $x = [13; \overline{1, 7}]$. Compute the value of x.

Solution: We have

$$x = [13; \overline{1, 7}] = 13 + \frac{1}{1 + \frac{1}{7 + \frac{1}{1 + \cdots}}},$$

thus we put

$$y = [\overline{1; 7}] = 1 + \frac{1}{7 + \frac{1}{1 + \frac{1}{7 + \cdots}}}.$$

Then $x = 13 + 1/y$, and furthermore

$$y = 1 + \frac{1}{7 + \frac{1}{y}} = 1 + \frac{y}{7y + 1}$$

so

$$(y - 1)(7y + 1) = y,$$

which has the solutions $y = \frac{1}{2} \pm \frac{\sqrt{77}}{14}$. Picking the positive solution we have that $y = \frac{1}{2} + \frac{\sqrt{77}}{14}$, and that

$$x = 13 + \frac{1}{y} = 13 + \frac{1}{\frac{1}{2} + \frac{\sqrt{77}}{14}} = \frac{105 + 13\sqrt{77}}{7 + \sqrt{77}}.$$

(There is no need to perform the last simplification.)

4) The function f satisfies

$$\begin{aligned}
f(1) &= 1 \\
f(1) + f(2) &= a \\
f(1) + f(3) &= b \\
f(1) + f(2) + f(4) &= c \\
f(1) + f(2) + f(3) + f(6) &= ab \\
f(1) + f(2) + f(3) + f(4) + f(6) + f(12) &= bc
\end{aligned}$$

Calculate $f(12)$. For which a, b, c can f be extended to a multiplicative function on the positive integers?

Solution: We can write this as

$$F(1) = \sum_{d|1} f(d) = 1$$
$$F(2) = \sum_{d|2} f(d) = a$$
$$F(3) = \sum_{d|3} f(d) = b$$
$$F(4) = \sum_{d|4} f(d) = c$$
$$F(6) = \sum_{d|6} f(d) = ab$$
$$F(12) = \sum_{d|12} f(d) = bc$$

By Möbius inversion, we get that

$$f(12) = \sum_{d|12} F(d)\mu(12/d) = 1*0 + a*1 + b*0 + c*(-1) + ab*(-1) + bc*1 = a - c - ab + bc.$$

Since $F(6) = ab = F(2) * F(3)$ and $F(12) = bc = F(3) * F(4)$, and since $2, 3, 4$ are primes or prime powers, F can be extended to a multiplicative function $\tilde{F}$ on all positive integers (by arbitrarily assigning values on the other prime powers). Then the function $\tilde{f} = \mu * \tilde{F}$ is also multiplicative, and extends f to all positive integers. This holds for all values of a, b, c.

5) Show that 10 is a primitive root modulo 17. List all quadratic residues mod 17.

Solution: By tedious calculations, we see that the order of 3 mod 17 is 16, hence 3 is a primitive root mod 17. Since

$$3^3 = 27 \equiv 10 \mod 17$$

and $\gcd(3, 16) = 1$, we have that 10 is another primitive root mod 17.

We have that an integer is a quadratic residue mod 17 iff it has even index w.r.t. the primitive root 10, which occurs iff it has even index w.r.t. the primitive root 3. We calculate (mod 17)

$$3^0 \equiv 3^{16} \equiv 1, \quad 3^2 \equiv 9, \quad 3^4 \equiv 13, \quad 3^6 \equiv 15, \quad 3^8 \equiv 16, \quad 3^{10} \equiv 8, \quad 3^{12} \equiv 4, \quad 3^{14} \equiv 2$$

so the quadratic residues mod 17 are

$$1, 2, 4, 8, 9, 13, 15, 16.$$

6) The number 41 is a prime. Show that -1 is a quadratic residue module 41, then find a solution to the congruence

$$x^2 \equiv -1 \mod 41$$

Among the solutions (m, n) to

$$mx + n \equiv 0 \mod 41$$

find a pair with $0 < |m|, |n| \leq 6$. Show that $41 = m^2 + n^2$.

Solution:

If we can find such m, n, x, then

$$n^2 = (-n)^2 \equiv m^2x^2 \equiv -m^2 \mod 41,$$

so $m^2 + n^2 \equiv 0 \mod 41$, hence $41|(m^2 + n^2)$. However, we have that $0 < m^2 + n^2 < 2 * 41$, so $m^2 + n^2 = 41$.

Since $41 \equiv 1 \mod 4$, we have that $\left(\frac{-1}{41}\right) = (-1)^{\frac{41-1}{2}} = 1$, so -1 is a quadratic residue mod 41. Listing the squares mod 41, we se that $7^2 \equiv 8 \mod 41$, $8^2 \equiv 23 \mod 41$, but $9^2 \equiv -1 \mod 41$, so the solutions to $x^2 \equiv -1 \mod 41$ are $x = \pm 9$. We pick $x = 9$.

The congruence

$$9m + n \equiv 0 \mod 41$$

is equivalent to the Diophantine equation

$$41k + 9m + n = 0$$

which has the solutions

$$(k, m, n) = (t, s, -41t - 9s), \qquad t, s \in \boldsymbol{Z}.$$

Picking $t = -1, s = 4$ gives $m = 4$,$n = 5$, satisfying $0 < |m|, |n| \leq 6$. We check that $4^2 + 5^2 = 15 + 25 = 41$.