Number theory, Talteori 6hp, Kurskod TATA54, Provkod TEN1
March 12, 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 textbooks.

1) Determine all solutions to $180x \equiv 120 \mod 240$.

2) Find all solutions to the congruence

$$x^7 + x^3 + x + 1 \equiv 0 \qquad \mod 16.$$

3) Consider the polynomial $f(t) = t^4 + 2t^2 - 4$. Does f have a zero which is an integer? A zero mod 19? A zero mod 43? Find examples of such zeroes, when possible.

4) Write 41 as a sum of two squares, and then write 205 as a sum of two squares. Finally, write 222 as a sum of four squares.

5) Find the continued fraction expansion of $\sqrt{17}$, then approximate $\sqrt{17}$ with a rational number, with an error less than 0.002.

6) Let$f$ be a multiplicative arithmetical function. If the argument n has prime factorization $n = p_1^{a_1} \cdots p_k^{a_k}$, show that

$$\sum_{d|n} \mu(d) f(d) = (1 - f(p_1)) \cdots (1 - f(p_k)).$$

Use this to show that

$$\sum_{d|n} \frac{\mu(d)}{d} = \frac{\phi(n)}{n}.$$

7) Determine all positive integer solutions to $x^2 + 2y^2 = z^2$.

Number theory, Talteori 6hp, Kurskod TATA54, Provkod TEN1
March 12, 2017
LINKÖPINGS UNIVERSITET
Matematiska Institutionen
Examinator: Jan Snellman

Solutions

1) Determine all solutions to $180x \equiv 120 \mod 240$.

Solution: Since $\gcd(180, 240) = 60$, this is equivalent to $3x \equiv 2 \mod 4$, which is equivalent to $x \equiv 3 * 2 \equiv 2 \mod 4$.

2) Find all solutions to the congruence

$$x^7 + x^3 + x + 1 \equiv 0 \qquad \mod 16.$$

Solution: Put $f(x) = x^7 + x^3 + x + 1$. Then $f(1) \equiv 0 \mod 2$, and $f'(x) = 7x^6 + 3x^2 + 1$, so $f'(1) \equiv 1 \not\equiv 0 \mod 2$, hence this solution lifts uniquely mod 2^n for all n.

Lift to 2^2: $f(1) = 4 \equiv 0 \mod 2^2$.

Lift to 2^3: $f(1) = 4 \not\equiv 0 \mod 2^3$.

$$\begin{aligned} 0 \equiv f(1 + 2^2 t) &\equiv f(1) + 2^2 f'(1)t \mod 2^3 \\ &\equiv 4 + 4 * 11t \mod 2^3 \\ &\equiv 4 + 4t \mod 8. \end{aligned}$$

So $t \equiv -1 \equiv 1 \mod 2$, and $r_1 = 1$ lifts to $r_2 = 1 + 4 * 1 = 5$.

Lift to 2^4: $r_2^3 \equiv r_2^7 \equiv 13 \mod 16$, so $f(r_2) \equiv 0 \mod 16$. Thus $r_3 = r_2 = 5$ is a solution mod 16.

3) Consider the polynomial $f(t) = t^4 + 2t^2 - 4$. Does f have a zero which is an integer? A zero mod 19? A zero mod 43? Find examples of such zeroes, when possible.

Solution: We write the equation $f(t) = 0$ as

$$(t^2 + 1)^2 = 5 \tag{1}$$

This shows that there are no integer solutions. Since

$$\left(\frac{5}{43}\right) = \left(\frac{43}{5}\right) = \left(\frac{3}{5}\right) = \left(\frac{5}{3}\right) = \left(\frac{2}{3}\right) = -1$$

the equation has no solution modulo 43.

On the other hand,

$$\left(\frac{5}{19}\right) = \left(\frac{19}{5}\right) = \left(\frac{-1}{5}\right) = 1,$$

so we can at least solve $u^2 \equiv 5 \mod 19$. In fact, the solutions are $u \equiv \pm 9 \mod 19$.

The equation $t^2 + 1 \equiv u \equiv 9 \mod 19$ is equivalent to $t^2 \equiv 8 \mod 19$. Since $8^9 \equiv -1 \mod 19$, the Euler Criteria gives that this equation has no solutions. On the other hand $t^2 + 1 \equiv u \equiv -9 \mod 19$ is equivalent to $t^2 \equiv -10 \equiv 9 \mod 19$. This has the solutions $t \equiv \pm 3 \mod 19$.

Thus, the solutions to $(t^2+1)^2 \equiv 5 \mod 19$ are precisely $t \equiv \pm 3 \mod 19$.

4) Write 41 as a sum of two squares, and then write 205 as a sum of two squares. Finally, write 222 as a sum of four squares.

Solution: Since $p \equiv 1 \mod 4$, we can use the method described in the lecture.

First, find a square root of -1 mod 41; $r = 9$ works.

Secondly, put $x = -r/p = -9/41$, and put $n = \lceil \sqrt{p} \rceil = 6$. We want to approximate x with a rational number a/b such that $b \leq n$ and

$$|x - a/b| \leq \frac{1}{b(n+1)} < \frac{1}{b\sqrt{p}}.$$

Thirdly, the continued fraction expansion of x is $[-1, 1, 3, 1, 1, 4]$, and the third convergent is $-1/5$. We put $a = -1$, $b = 5$ and $c = rb + pa = 9 * 5 + 41 * (-1) = (-4)$. Then $b^2 + c^2 = 5^2 + (-4)^2 = 25 + 36 = 41$.

Finally, we can express $41 = 4^2 + 5^2$. For this small prime, we could have found this easily by exhaustive search.

Now note that $205 = 41 * 5$. Since $5 = 2^2 + 1$, we can write

$$205 = N(4 + 5i)N(2 + i) = N((4 + 5i)(2 + i)) = N(3 + 14i),$$

hence $205 = 3^2 + 14^2$.

Since $17 = 4^2 + 1^2$, it follows that $222 = 205 + 17 = 3^2 + 14^2 + 4^2 + 1^2$.

5) Find the continued fraction expansion of $\sqrt{17}$, then approximate $\sqrt{17}$ with a rational number, with an error less than 0.002.

Solution: We get that $\sqrt{17} = [4, \overline{8}]$ and that the successive convergents are

$$c_0 = 4, \quad , c_1 = 33/8, \quad c_2 = 268/65.$$

Since $c_2 < \sqrt{17} < c_1$ and $c_1 - c_2 = 1/520 < 2/1000$, we have that $|\sqrt{17} - 33/8| < 0.002$, as desired.

6) Let$f$ be a multiplicative arithmetical function. If the argument n has prime factorization $n = p_1^{a_1} \cdots p_k^{a_k}$, show that

$$\sum_{d|n} \mu(d) f(d) = (1 - f(p_1)) \cdots (1 - f(p_k)).$$

Use this to show that

$$\sum_{d|n} \frac{\mu(d)}{d} = \frac{\phi(n)}{n}.$$

Solution: : This is two exercises in chapter 7 in the textbook.

7) Determine all positive integer solutions to $x^2 + 2y^2 = z^2$.

Solution: This is an exercise in chapter 13 in the textbook.