Elementär Talteori: 2012-08-25

Hjälpmedel: Papper och skrivdon.

1. Find all pythagorean triples which have 18 as one of their components!

   Solution: We look for primitive pythagorean triples $(p^2 - q^2, 2pq, p^2 + q^2)$ with $p > q, \gcd(p,q) = 1, 2|pq$, where one of the components is a divisor of 18 and then multiply with $\frac{18}{d}$. One checks easily that $d = p^2 + q^2$ is impossible.

   (a) $d = 1, 2$ is impossible.

   (b) $d = 3 \Longrightarrow 3 = p^2 - q^2 = (p+q)(p-q) \Longrightarrow p = 2, q = 1$. So we obtain $6 \cdot (3,4,5) = (18,24,30)$.

   (c) $d = 6 \Longrightarrow 6 = 2pq$, which is impossible, since pq is even.

   (d) $d = 9 \Longrightarrow 9 = (p+q)(p-q) \Longrightarrow p = 5, q = 4$. So we obtain $2 \cdot (9,40,41) = (18,80,82)$.

   (e) $d = 18 \Longrightarrow 18 = 2pq$, which is impossible, since pq is even.

2. Show that there is no integer solution $(x,y) \in \mathbb{Z}^2$ of the equation

$$6x^2 - 11y^4 = 47.$$

   Solution: If there is a solution in $\mathbb{Z}$, then as well in $\mathbb{Z}_n$ for every $n \in \mathbb{N}$. We take $n = 11$ and may forget about $11y^4$. It follows that

$$\overline{6}^{-1} \cdot \overline{47} \in \mathbb{Z}_{11}$$

   is a square. If so, we have

$$1 = \left(\frac{6 \cdot 47}{11}\right) = \left(\frac{2}{11}\right)\left(\frac{3}{11}\right)\left(\frac{3}{11}\right) = -1,$$

   a contradiction!

3. Solve the congruence $108x \equiv 171 \mod (529)$.

   Solution:

   (a) $108x = 171 + 529y$

   (b) $529y \equiv 171 \mod (108)$

(c) $-11y \equiv 45 \mod (108)$

(d) $-11y = 45 + 108z$

(e) $108z \equiv -45 \mod (11)$

(f) $-2z \equiv -1 \mod (11)$

If we take $z = -5$, we obtain $y = 45$ and $x = 222$. So $x \equiv 222 \mod (529)$ is the solution.

4. (a) Find the least positive solution of the simultaneous congruences

$$x \equiv 5 \mod (12), x \equiv 17 \mod (20), x \equiv 23 \mod (42).$$

Solution: The above congruences are equivalent to four congruences with prime power moduli

$$x \equiv 2 \mod (3), x \equiv 1 \mod (4), x \equiv 2 \mod (5), x \equiv 2 \mod (7).$$

or

$$x \equiv 1 \mod (4), x \equiv 2 \mod (105).$$

Then we consider the following chinese remainder table:

$\mathbb{Z}_{420}$	$\mathbb{Z}_4 \times \mathbb{Z}_{105}$
$\overline{105}$	$(\overline{1}, \overline{0})$
$-\overline{104}$	$(\overline{0}, \overline{1})$
$-\overline{103}$	$(\overline{1}, \overline{2})$

,

Thus the least positive solution of our congruences is $x = -103 + 420 = 317$.

(b) Solve the congruence $x^6 - 2x^5 - 35 \equiv 0 \mod (125)$.

Solution: We are hunting for zeros of $f = X^6 - 2X^5 - 35 \in \mathbb{Z}[X]$ in $\mathbb{Z}_{125}$.

i. We have $\overline{f} = X^6 - 2X^5 = X^5(X-2) \in \mathbb{Z}_5[X]$. Hence $x = \overline{0}, \overline{2}$. Furthermore $f' = 6X^5 - 10X^4$ satisfies $f'(\overline{0}) = 0$ and $f'(\overline{2}) = \overline{2}$. So there is a unique lift of $x = \overline{2}$ to $\mathbb{Z}_{125}$, while for $x = \overline{0}$ we have to see.

ii. In $\mathbb{Z}_{25}$ we consider $y = t \cdot \overline{5}, \overline{2} + t \cdot \overline{5}$. The congruences to be satisfied by t are

$$0 \cdot t \equiv -7 \mod (5) \text{ resp. } 2 \cdot t \equiv -3 \mod (5)$$

The first one is unsolvable, the second one has the solution $t = 1$. So in $\mathbb{Z}_{25}$ there is only one zero, namely $y = \overline{7}$.

iii. In $\mathbb{Z}_{125}$ we have $z = \overline{7} + t \cdot \overline{25}$, where t satisfies

$$2 \cdot t \equiv 0 \mod (5),$$

so $z = \overline{7} \in \mathbb{Z}_{125}$.

5. Determine all natural numbers such that there are exactly 8 primitive roots in $\mathbb{Z}_m^*$.

Solution: First of all the only integers m, such that $\mathbb{Z}_m^*$ admits a primitive root are $m = 2, 4, p^r, 2p^r$ with an odd prime p. Since $\mathbb{Z}_m^* \cong \mathbb{Z}_{2m}^*$ for odd m, we may assume $m = p^r$. Now if a is a primitive root, then a power a^k is a primitive root iff $\gcd(k, \varphi(m)) = 1$. So there are $\varphi(\varphi(m))$ primitive roots. We distinguish three cases:

(a) $m = p^r, r \geq 3$: In that case we have $\varphi(\varphi(m)) = \varphi(p^{r-1}(p-1)) = p^{r-2}(p-1)\varphi(p-1)$, so p divides 8 - but that is absurd.

(b) $m = p^2$: In that case we have $\varphi(\varphi(m)) = \varphi(p(p-1))$ $= (p-1)\varphi(p-1)$, so $p-1$ divides 8 and thus $p = 3, 5$. Obviously only $p = 5$ resp. $m = 25$ is a solution.

(c) $m = p$: For a prime divisor q of $p-1$ the number $q-1$ is a divisor of 8, hence $q = 2, 3, 5$, and $p - 1 = 5^k 3^\ell 2^n$ with $k, \ell \leq 1$. For $k = \ell = 1$ we have the possibilities $n = 0, 1$. If $n = 0$, we find $p = 16$ - impossible, but $n = 1$ gives $p = m = 31$. Now if $p - 1 = 5 \cdot 2^n$, we have $n = 2$ and $p = 21$, impossible as well. The case $p - 1 = 3 \cdot 2^n$ leads to $n = 3$ resp. $p = 25$, impossible! Finally $p - 1 = 2^n$ gives $n = 4$ and $p = 17$, a further solution!

6. Find the value of the continued fraction $K(5, \overline{7, 3})$!

Solution: We have $K(5, \overline{7, 3}) = 5 + \frac{1}{y}$, where $x := K(\overline{7, 3})$ satisfies

$$y = K(7, 3, y) = 7 + \frac{1}{3 + \frac{1}{x}} \iff 3y^2 - 21y - 7 = 0, y > 7 \iff y = \frac{7}{2} + \frac{5}{6}\sqrt{21}.$$

Finally

$$K(5,\overline{7,3}) = 5 + \frac{1}{y} = \frac{1}{42}(147 + 15\sqrt{21}).$$

7. Find a primitive root a for the group of units $(\mathbb{Z}[\sqrt{6}])^*$ of the ring $\mathbb{Z}[\sqrt{6}]$, i.e. such that $\mathbb{Z}[\sqrt{6}]^* = \{\pm a^n; n \in \mathbb{Z}\}$, or equivalently, determine a fundamental solution for the equations $x^2 - 6y^2 = \pm 1$.

   Solution: Obviously $a = 5+2\sqrt{6}$ it is a unit. Indeed is the basic unit, since there is no unit $\alpha + \beta\sqrt{6}$ with $\alpha < 5, \beta < 2$.

8. Compute $\left(\frac{461}{773}\right)$.

   Solution: Both 461 and 773 are primes, hence

$$\left(\frac{461}{773}\right) = \left(\frac{773}{461}\right) = \left(\frac{461}{773}\right) = \left(\frac{-149}{461}\right) = \left(\frac{-1}{461}\right)\left(\frac{149}{461}\right)$$

$$\left(\frac{461}{149}\right) = \left(\frac{14}{149}\right) = \left(\frac{2}{149}\right)\left(\frac{7}{149}\right) = -\left(\frac{149}{7}\right) = -\left(\frac{2}{7}\right) = -1.$$