Uppsala Universitet
Matematiska Institutionen
Andreas Strömbergsson

Prov i matematik
Elementär talteori
2016-03-15

Skrivtid: 14.00 – 19.00.
Tillåtna hjälpmedel: Papper, skrivdon och miniräknare.

1. Solve the Diophantine equations

(a) $18x + 12y = 24$;

(b) $15x - 12y + 20z = 7$. (5p)

2. Determine the zeros of the following polynomials:

(a) $X^3 - 2$ in $\mathbb{Z}_{125}$;

(b) $X^2 - X$ in $\mathbb{Z}_{99}$;

(c) $X^5 + X^4 + 4$ in $\mathbb{Z}_{16}$.

(6p)

3. Determine whether the following residue classes are squares:

(a) $\overline{485}$ in $\mathbb{Z}_{743}$.

(b) $\overline{743}$ in $\mathbb{Z}_{485}$.

(5p)

4. (a) Prove that $\overline{3}$ is a primitive root in $\mathbb{Z}_{17}^{\times}$.

(b) Determine all elements of order 4 in $\mathbb{Z}_{17}^{\times}$.

(5p)

5. Find all Pythagorean triples which have 16 as one of their components!

(5p)

6. (a) Find the continued fraction expansion of $\sqrt{18}$ and compute its first three convergents.

(b) Find two solutions $(x, y) \in \mathbb{N}^2$ to the equation $x^2 - 18y^2 = 1$.

(c) Are there any solutions $(x, y) \in \mathbb{N}^2$ to the equation $x^2 - 18y^2 = -1$?

(5p)

7. Compute the value of the continued fraction expansion $\langle 1, \overline{2, 7} \rangle$!

(4p)

8. (a) Assume that m_1, m_2 are positive integers which are not relatively prime, and let x be any integer. Prove that there exists some integer y which satisfies

$$y \equiv x \pmod{m_1}, \quad y \equiv x \pmod{m_2}, \quad \text{and } y \not\equiv x \pmod{m_1 m_2}.$$

(b) Let a and $g > 0$ be given integers. Prove that there exist integers x, y satisfying

$$(x, y) = g \qquad \text{and} \qquad xy = a,$$

if and only if $g^2 \mid a$.

(5p)

LYCKA TILL / GOOD LUCK!

Solutions

1. We use the same method of presentation as in MNZ p. 218 (top).

(a).

$$\begin{pmatrix} 18 & 12 & 24 \\ 1 & 0 & \\ 0 & 1 & \end{pmatrix} \to \begin{pmatrix} 6 & 12 & 24 \\ 1 & 0 & \\ -1 & 1 & \end{pmatrix} \to \begin{pmatrix} 6 & 0 & 24 \\ 1 & -2 & \\ -1 & 3 & \end{pmatrix}$$

Answer: $(x, y) = (4 - 2s, -4 + 3s)$, $s \in \mathbb{Z}$. (Replacing s by $s = 2 - k$ we obtain the slightly nicer answer $(x, y) = (2k, 2 - 3k)$, $k \in \mathbb{Z}$.)

(b).

$$\begin{pmatrix} 15 & -12 & 20 & 7 \\ 1 & 0 & 0 & \\ 0 & 1 & 0 & \\ 0 & 0 & 1 & \end{pmatrix} \to \begin{pmatrix} 3 & -12 & -4 & 7 \\ 1 & 0 & 0 & \\ 1 & 1 & 2 & \\ 0 & 0 & 1 & \end{pmatrix} \to \begin{pmatrix} 3 & 0 & -1 & 7 \\ 1 & 4 & 1 & \\ 1 & 5 & 3 & \\ 0 & 0 & 1 & \end{pmatrix}$$

$$\to \begin{pmatrix} 0 & 0 & -1 & 7 \\ 4 & 4 & 1 & \\ 10 & 5 & 3 & \\ 3 & 0 & 1 & \end{pmatrix}.$$

Answer: $(x, y, z) = (-7 + 4s + 4t, -21 + 10s + 5t, -7 + 3s)$, $s, t \in \mathbb{Z}$.

2. (a) The prime factorization of 125 is $125 = 5^3$.

Set $f(X) = X^3 - 2 \in \mathbb{Z}[X]$. Note that the only solution to $f(X) \equiv 0 \bmod 5$ is $X \equiv 3 \bmod 5$. We have $f'(X) = 3X^2$ and $f'(3) = 3 \cdot 3^2 = 27$ which is not divisible with 5; hence by Hensel's Lemma, $3 \bmod 5$ lifts to a unique solution modulo 25. and then to a unique solution modulo 125. To determine the lift modulo 25, let $t \bmod 5$ be the unique solution to $f'(3)t \equiv -f(3)/5 \bmod 5$, i.e. $2t \equiv -5 \bmod 5$, i.e. $t \equiv 0 \bmod 5$; then the formula in Hensel's Lemma says that $b = 3 + 5 \cdot 0 = 3$ is the unique lift $\bmod 25$ of the solution $3 \bmod 5$. Next, to determine the lift modulo 125, let $t \bmod 5$ be the unique solution to $f'(3)t \equiv -f(3)/5^2 \bmod 5$, i.e. $2t \equiv -1 \bmod 5$, i.e. $t \equiv 2 \bmod 5$; then the formula in Hensel's Lemma says that $b = 3 + 25 \cdot 2 \equiv 53 \bmod 125$ is the unique lift $\bmod 125$ of the solution $3 \bmod 25$.

Answer: There is exactly one zero, namely $X \equiv 53 \bmod 125$.

(b) The prime factorization of 99 is $99 = 3^2 \cdot 11$. Note that $X^2 - X = (X - 1)X$ in $\mathbb{Z}[X]$; hence we can immediately solve the congruence equation modulo 9 and modulo 11. Indeed, if $(X-1)X \equiv 0 \bmod 9$ then $X-1$ or X must be divisible by 3, i.e. $X \equiv 0$ or $1 \bmod 3$. Then the *other* factor ($X - 1$ or X) is certainly *not* divisible by 3, and hence the only possibility for $(X-1)X \equiv 0 \bmod 9$ is if $X \equiv 0$ or $1 \bmod 9$. Similarly (but more easily) the only two solutions of $(X-1)X \equiv 0 \bmod 9$ are $X \equiv 0$ or $1 \bmod 11$.

Now we use the Chinese Remainder Theorem to determine all the solutions mod 99. We first seek $a, b \in \mathbb{Z}$ so that $9a + 11b = 1$; we find $a = 5$, $b = -4$ by simple trying (or using Euclid's Algorithm). From this we find the number $9 \cdot 5 = 45$ which is $\equiv 0 \bmod 9$ and $\equiv 1 \bmod 11$, and we also find the number $11 \cdot (-4) = -44$ which is $\equiv 1 \bmod 9$ and $\equiv 0 \bmod 11$. Hence for any $x, y \in \mathbb{Z}$, the unique integer mod 99 which is $\equiv x \bmod 9$ and $\equiv y \bmod 11$ equals $-44x + 45y$. Applying this to the solutions of the given equation mod 9 and mod 11, we see that there are the following four solutions mod 99:

$$0 \cdot (-44) + 0 \cdot 45 = 0; \qquad 1 \cdot (-44) + 0 \cdot 45 = -44 \equiv 55;$$
$$0 \cdot (-44) + 1 \cdot 45 = 45; \qquad 1 \cdot (-44) + 1 \cdot 45 = 1.$$

Answer: $\overline{0}$, $\overline{1}$, $\overline{45}$ and $\overline{55}$.

(c) The prime factorization of 16 is $16 = 2^4$. Set $f(X) = X^5 + X^4 + 4 \in \mathbb{Z}[X]$. Note that the solutions to $f(X) \equiv 0 \bmod 2$ are both $X \equiv 0$ and $1 \bmod 2$. We compute $f'(X) = 5X^4 + 4X^3 \in \mathbb{Z}[X]$, and note that $f'(0) \equiv 0 \bmod 2$ but $f'(1) \equiv 1 \bmod 2$. Hence by Hensel's Lemma, $1 \bmod 2$ lifts to a unique solution modulo 16, while $0 \bmod 2$ lifts to either 0 or 2 solutions modulo 4, etc. We compute that $f(0) = 4 \equiv 0 \bmod 4$; hence in fact $0 \bmod 2$ lifts to the two solutions $0 \bmod 4$ and $2 \bmod 4$. However none of these lift to any solution modulo 8, since $f(0) \equiv 4 \not\equiv 0 \bmod 8$ and $f(2) \equiv 4 \not\equiv 0 \bmod 8$.

To compute the lift of $1 \bmod 2$, let $t \bmod 2$ be the unique solution to $f'(1)t \equiv -f(1)/2 \bmod 2$, i.e. $t \equiv 1 \bmod 2$; then the formula in Hensel's Lemma says that $b = 1 + 2 \cdot 1 = 3$ is the unique lift $\bmod 4$ of the solution $1 \bmod 2$. Next let $t \bmod 2$ be the unique solution to $f'(1)t \equiv -f(3)/4 \bmod 2$ (note $f(3) = 328 \equiv 0 \bmod 8$), that is $t \equiv 0 \bmod 2$; then the formula in Hensel's Lemma says that $b = 3 + 4 \cdot 0 = 3$ is the unique lift $\bmod 8$ of the solution $3 \bmod 4$. Finally let $t \bmod 2$ be the unique solution to $f'(1)t \equiv -f(3)/8 \bmod 2$ (note $f(3) = 328 \equiv 8 \bmod 16$), that is $t \equiv 1 \bmod 2$; then the formula in Hensel's Lemma says that $b = 3 + 8 \cdot 1 = 11$ is the unique lift $\bmod 16$ of the solution $3 \bmod 8$.

Answer: There is exactly one solution, $X = 11 \bmod 16$.

3. (a) No: 743 is a prime and we compute

$$\left(\frac{485}{743}\right) = \left(\frac{5}{743}\right)\cdot\left(\frac{97}{743}\right) = \left(\frac{743}{5}\right)\cdot\left(\frac{743}{97}\right) = \left(\frac{3}{5}\right)\cdot\left(\frac{64}{97}\right)$$
$$= (-1)\left(\frac{2}{97}\right)^6 = -1.$$

(b) No: $485 = 5 \cdot 97$ and 743 is not a square mod 5.

4. (a) $p = 17$ is a prime and $\phi(p) = p - 1 = 16 = 2^4$. Let h be the order of $\overline{3}$ in $\mathbb{Z}_{17}$. By Fermat's Little Theorem, $\overline{3}^{16} = \overline{1}$; hence $h \mid 16$. Therefore, if $h \neq 16$, then we must have $h \mid 8$, and this would imply $\overline{3}^8 = \overline{1}$. Hence if we check that $\overline{3}^8 \neq \overline{1}$ then it follows that $h = 16$ and therefore that $\overline{3}$ is a primitive root in $\mathbb{Z}_{17}$. We compute in $\mathbb{Z}_{17}$: $\overline{3}^3 = \overline{27} = -\overline{7}$; $\overline{3}^6 = (-\overline{7})^2 = \overline{49} = -\overline{2}$; $\overline{3}^8 = -\overline{2}\cdot\overline{3}^2 = -\overline{1}$. This is $\neq \overline{1}$, and hence we have proved that $\overline{3}$ is a primitive root in $\mathbb{Z}_{17}$.

(b) The elements of $\mathbb{Z}_{17}^\times$ are $\overline{3}^j$ for $j \in \mathbb{Z}$, $j \pmod{16}$, and $\overline{3}^j$ has order $16/(16, j)$, by MNZ Lemma 2.33 (cf. the beginning of Lecture #6). Hence $\overline{3}^j$ has order 4 iff

$$\begin{aligned} &16/(16, j) = 4 \\ &\Leftrightarrow (16, j) = 4 \\ &\Leftrightarrow [4 \mid j \text{ and } (4, j/4) = 1] \\ &\Leftrightarrow j \equiv 4 \text{ or } 12 \pmod{16}. \end{aligned}$$

Hence there are exactly two elements of order 4 in $\mathbb{Z}_{16}^\times$, namely $\overline{3}^4 = \overline{81} = \overline{13}$ and $\overline{3}^{12} = \overline{3}^{-4} = \overline{13}^{-1} = -\overline{13}$. (The last equality is easiest seen as follows: Since $\overline{13}$ has order 4, we must have $\overline{13}^2 = -\overline{1}$; hence $\overline{13}^{-1} = -\overline{13}$.)

Answer: $\overline{13}$ and $\overline{4}$.

5. We search all primitive Pythagorean triples $\langle 2rs, r^2 - s^2, r^2 + s^2\rangle$ with $r > s > 0$ and $\gcd(r, s) = 1$ and $r \not\equiv s \bmod 2$, where one of the components equals d, a divisor of 16 (thus: $d \in \{1, 2, 4, 8, 16\}$), and then multiply with $16/d$. Now one notes that there are no solutions with $d = 1$ or $d = 2$ (proof: $r > s > 0$ implies $r^2 + s^2 > r^2 - s^2 = (r - s)(r + s) \geq 1 \cdot 3 = 3$ and $2rs \geq 4$). Hence from now on we assume $d = 4$ or $d = 8$ or $d = 16$, i.e. $d = 2^j$ with $j \in \{2, 3, 4\}$. Note that $r \not\equiv s \bmod 2$ implies that $r^2 - s^2$ and $r^2 + s^2$ are odd; hence the only possibility is $2rs = d = 2^j$, i.e. $rs = 2^{j-1}$. Now by assumption one of r, s is odd; and from $rs = 2^{j-1}$ it follows that the odd number among r, s is not divisible by *any* prime; hence it must be equal to 1; and using $r > s$ we conclude that this number must be s; thus $s = 1$ and $r = 2^{j-1}$. Conversely we see that this choice of r, s works; it gives the Pythagorean triple $\langle 2^j, 2^{2j-2} - 1, 2^{2j-2} + 1\rangle$, and multiplying with $16/d = 2^{4-j}$ we obtain the Pythagorean triple $\langle 16, 2^{j+2} - 2^{4-j}, 2^{j+2} + 2^{4-j}\rangle$.

Answer: There are exactly three such triples, namely

$$\langle 16, 2^{j+2} - 2^{4-j}, 2^{j+2} + 2^{4-j}\rangle \qquad \text{for } j \in \{2, 3, 4\};$$

or with numbers: $\langle 16, 12, 20\rangle$ and $\langle 16, 30, 34\rangle$ and $\langle 16, 63, 65\rangle$. (This is disregarding the obvious possibility to switch the first two components; otherwise of course there are *six* triples: $\langle 16, 12, 20\rangle$ and $\langle 12, 16, 20\rangle$ and $\langle 16, 30, 34\rangle$ and $\langle 30, 16, 34\rangle$ and $\langle 16, 63, 65\rangle$ and $\langle 63, 16, 65\rangle$.)

6. (a). We follow the algorithm from Lecture 12. Note that if we set $d = 18$, $u_0 = 0$, $v_0 = 1$, then $\sqrt{18} = \frac{u_0+\sqrt{d}}{v_0}$ and $v_0 \mid d - u_0^2$. Next we compute a_j for $j \geq 0$ and u_j, v_j for $j \geq 1$ using the recursion formulas $a_j = \left[\frac{u_j+\sqrt{d}}{v_j}\right]$, $u_{j+1} = a_j v_j - u_j$, $v_{j+1} = (d - u_{j+1}^2)/v_j$. We get:

j	0	1	2	3
u_j	0	4	4	4
v_j	1	2	1	2
a_j	4	4	8	

Thus $\sqrt{18} = \langle 4, \overline{4, 8} \rangle$.

We compute the convergents using the formulas $h_{-2} = 0$, $h_{-1} = 1$, $h_j = a_j h_{j-1} + h_{j-2}$ and $k_{-2} = 1$, $k_{-1} = 0$, $k_j = a_j k_{j-1} + k_{j-2}$.

j	-2	-1	0	1	2	3
a_j			4	4	8	
h_j	0	1	4	17	140	
k_j	1	0	1	4	33	

Answer: $\sqrt{18} = \langle 4, \overline{4, 8} \rangle$, and the first three convergents are
$\dfrac{h_0}{k_0} = \dfrac{4}{1}, \dfrac{h_1}{k_1} = \dfrac{17}{4}, \dfrac{h_2}{k_2} = \dfrac{140}{33}$.

(b). Since $\sqrt{18} = \langle 4, \overline{4, 8} \rangle$ with period $r = 2$, the first solution is given by $\langle x, y \rangle = \langle h_{r-1}, k_{r-1} \rangle = \langle 17, 4 \rangle$. Computing $(17 + 4\sqrt{18})^2 = 17^2 + 16 \cdot 18 + 136\sqrt{17} = 577 + 136\sqrt{17}$ we find a second solution $\langle 577, 136 \rangle$.
Answer: $\langle 17, 4 \rangle$ and $\langle 577, 136 \rangle$.

(c). **Answer:** No, since $\langle 4, \overline{4, 8} \rangle$ has even period $r = 2$.

7. We first compute $x = \langle \overline{2,7} \rangle$. Note that

$$x = \langle 2, 7, x \rangle = 2 + \frac{1}{7 + \frac{1}{x}} = 2 + \frac{x}{7x+1} = \frac{15x+2}{7x+1};$$

hence $7x^2 - 14x - 2 = 0$, and so

$$x = 1 \pm \frac{3}{7}\sqrt{7}.$$

Here choosing the minus sign would lead to $x < 1$, contradicting $x = \langle 2, 7, \cdots \rangle > 2$; hence

$$x = 1 + \frac{3}{7}\sqrt{7}.$$

It follows that

$$\langle 1, \overline{2,7} \rangle = 1 + \frac{1}{x} = 1 + \frac{1}{1 + \frac{3}{7}\sqrt{7}} = 1 + \frac{1 - \frac{3}{7}\sqrt{7}}{1 - (\frac{3}{7})^2 \cdot 7} = 1 + \frac{7 - 3\sqrt{7}}{7 - 9}$$

$$= 1 + \frac{-7 + 3\sqrt{7}}{2} = -\frac{5}{2} + \frac{3}{2}\sqrt{7}.$$

Answer: $\langle 1, \overline{2,7} \rangle = -\frac{5}{2} + \frac{3}{2}\sqrt{7}$.

8. (a). Let $d = (m_1, m_2)$; then $d > 1$ by assumption. Now set

$$y = x + \frac{m_1 m_2}{d}.$$

Note that $\frac{m_1 m_2}{d}$ is divisible by both m_1 and m_2, since both $\frac{m_1}{d}$ and $\frac{m_2}{d}$ are integers. Hence $y \equiv x \bmod m_1$ and $y \equiv x \bmod m_2$. On the other hand we have $1 \leq \frac{m_1 m_2}{d} < m_1 m_2$ since $d > 1$; hence $\frac{m_1 m_2}{d}$ is not divisible by $m_1 m_2$, and therefore $y \not\equiv x \bmod m_1 m_2$. □

(b) (This is MNZ, p. 18, Problem 30.) First assume that x and y are integers satisfying $(x, y) = g$ and $xy = a$. Set $x_1 = x/g$ and $y_1 = y/g$; these are integers satisfying $(x_1, y_1) = 1$ and $x_1 y_1 = a/g^2$. The last relation shows that $g^2 \mid a$.

Conversely, if $g^2 \mid a$ then (following the previous discussion) we may take e.g. $x_1 = a/g^2$ and $y_1 = 1$; then $(x_1, y_1) = 1$ and $x_1 y_1 = a/g^2$, and therefore if we set $x = g x_1 = a/g$ and $y = g y_1 = g$ then $(x_1, y_1) = g$ and $xy = a$. □