Solutions to Number theory, Talteori 6hp, Kurskod TATA54, Provkod TEN1
June 4, 2019
LINKÖPINGS UNIVERSITET
Matematiska Institutionen
Examinator: Jan Snellman

1) Find all $(x, y) \in \mathbf{Z}^2$ such that (x, y) is a solution to $3x - 7y = 1$, and x, y are relatively prime.

   Solution: By Bezout, if $3x - 7y = 1$ then $\gcd(x, y) = 1$, thus any solution pair will be relatively prime.

   We have that $\gcd(x, y) = 1$ and that $3 * (-2) - 7 * (-1) = 1$, so the set of solutions are $(x, y) = (-2, -1) + n(-7, -3)$.

2) Write, if possible, 6! as a sum of two squares.

   Solution: $6! = 2 * 3 * 4 * 5 * 6 = 2^4 * 3^2 * 5 = 720$, which factors over the Gaussian Integers as

$$6! = (1 + i)^4 * 3^2 * (1 + 2i)(1 - 2i) = 2^2 * 3 * (1 + 2i) \quad \times \quad 2^2 * 3 * (1 - 2i)$$

   The norm of the first factor is $12^2 * (1 + 2^2) = 12^2 + 24^2 = 720$.

3) Show that

$$\frac{10}{7} < \sqrt[3]{3} < \frac{13}{9} < \frac{3}{2}$$

   and that if

$$\frac{10}{7} < \frac{a}{b} < \sqrt[3]{3} < \frac{c}{d} < \frac{3}{2}$$

   with $a, b, c, d \in \mathbf{N}$ then $b > 7$, $d > 2$.

   Solution: By cubing,

$$\frac{10}{7} < \sqrt[3]{3} < \frac{13}{9} \quad \iff \quad \frac{1000}{343} < 3 < \frac{2197}{729}$$

   which is true.

   Put $\alpha_0 = \alpha = \sqrt[3]{3}$. Then $1 < 10/7 < \alpha_0 < 3/2 < 2$, so $a_0 = 1$, $\alpha_1 = \frac{1}{\alpha_0 - 1} = \frac{1}{\sqrt[3]{3}-1}$. Then $2 < \alpha_1 < 7/3$, so $a_1 = 2$, $\alpha_2 = \frac{1}{\alpha_1 - a_1} = \frac{1}{\frac{1}{\sqrt[3]{3}-1} - 2}$.

   In fact, it is easy to show that $9/4 < \alpha_1 < 7/3$. Once we have proved this, it follows that $1/4 < \alpha_1 - 1 < 1/3$, so $3 < \frac{1}{\alpha_1 - 2} = \alpha_2 < 4$, so $a_2 = 3$.

   Thus, the CF expansion of $\sqrt[3]{3}$ starts as $[1, 2, 3, \ldots]$, and the first convergents are $1, 3/2, 10/7$. Since no rational numbers can approximate $\sqrt[3]{3}$ better than the convergent, except by having larger denominators, the assertion follows.

   So, how to prove that $9/4 < \alpha_1$? This follows since $\alpha_0 < 13/9$, hence $\alpha_0 - 1 < 4/9$, hence $\alpha_1 > 9/4$.

4) $(x, y) = (10, 3)$ is a positive solution to Pell's equation $x^2 - 11y^2 = 1$. Find another!

   Solution:

$$(10 + 3\sqrt{11})^2 = 199 + 60\sqrt{11},$$

   so $(x, y) = (199, 60)$ is another solution.

5) Let $f(x) = x^2 - x + 1$. Show that, modulo 7, both zeroes of $f(x)$ are primitive roots. Determine the number of zeroes of $f(x)$ modulo 7^n for all $n \geq 2$.

Solution: $3, 5$ are the zeroes mod 7. A direct calculation shows that they have multiplicative order 6. Since $f'(x) = 2x - 1$, we calculate $2*3-1 = 5$, $2*5-1 = 9$, both non-congruent to 7. Hensel's lemma yields that both zeroes lift uniquely to a zero mod 7^n for any positive n; consequently, there are exactly 2 zeroes mod 7^n.

6) Define the arithmetical function f by

$$f(n) = \sum_{d|n} \frac{\mu(d)}{d},$$

where μ is the Möbius function. Is f multiplicative? Denote by $\mathrm{Supp}(n)$ the set of primes dividing n. Does the value of $f(n)$ depend only on $\mathrm{Supp}(n)$?

Solution: : Let $F(d) = 1/d$. Then F is multiplicative. Since $f = \mu * F$, f is also multiplicative.

We calculate $f(p^a)$ where p is prime. Then

$$f(p^a) = \sum_{\ell=0}^{a} \mu(p^\ell)/\ell = \mu(1)/1 + \mu(p)/p = 1 - 1/p.$$

So

$$f(p_1^{a_1} \cdots p_r^{a_r}) = \prod_{j=1}^{r} f(p_j^{a_j}) = \prod_{j=1}^{r} (1 - 1/p_j)$$

which depends on the p_i's making up the support, but not the a_i's, the exponents.

7) Show that the polynomial $f(x) = x^4 + 1$ does not factor over $\mathbf{Z}$, i.e., can not be written as a product $f(x) = a(x)b(x)$ with both $a(x), b(x)$ of lower degree, yet $f(x)$ factors modulo any prime!

(Hint: consider the cases $p = 2$, $p \equiv 1, 5 \mod 8$, $p \equiv 7 \mod 8$, $p \equiv 3 \mod 8$)

Solution: : The polynomial has no real zeroes, hence no linear factors over $\mathbf{R}$. A case-by-case study shows that it cannot be written as $x^4 + 1 = (x^2 + ax + b)(x^2 + cx + d)$ with $z, b, c, d \in \mathbf{Z}$. It is thus irreducible over $\mathbf{Z}$.

Over $\mathbf{Z}_2$, $x^4 + 1 = (x + 1)^4$.

Now let p be an odd prime, and consider $f(x) \in \mathbf{Z}_p[x]$.

If $p \equiv 1 \mod 4$ then $\left(\frac{-1}{p}\right) = 1$, so -1 has a square root, say $q^2 = -1$. Then $x^4 + 1 = (x^2 - q)(x^2 + q)$.

If $p \equiv 7 \mod 8$, $\left(\frac{2}{q}\right) = 1$, so $2 = q^2$ for some q, and $x^4 + 1 = (x^2 - \frac{2}{q}x + 1)(x^2 + \frac{2}{q}x + 1)$.

If $p \equiv 3 \mod 8$, $\left(\frac{-2}{q}\right) = \left(\frac{-1}{q}\right)\left(\frac{2}{q}\right) = (-1)(-1) = 1$, so $-2 = q^2$ for some q, and $x^4 + 1 = (x^2 - \frac{2}{q}x - 1)(x^2 + \frac{2}{q}x - 1)$.