Elementaire Getaltheorie, 27-1-2004

1. Bepaal alle $x \in \mathbb{Z}$ die tegelijkertijd voldoen aan de beide volgende vergelijkingen,

$$\begin{aligned} x^2 &\equiv 9 \pmod{100} \\ 37x &\equiv 4 \pmod{85} \end{aligned}$$

2. (a) Voor welke priemgetallen is -3 een kwadraatrest ?

   (b) Zij $p > 3$ een priemgetal zó dat $q = 2p + 1$ priem is. Bewijs dat -3 een primitieve wortel modulo q is.

3. Stel $x \in \mathbb{N}$ en zij p een priemdeler van $x^4 + x^3 + x^2 + x + 1$.

   (a) Bewijs dat $p \equiv 1 \pmod 5$ of $p = 5$. (Hint: merk op dat $x^4 + x^3 + x^2 + x + 1 = \frac{x^5-1}{x-1}$.)

   (b) Bewijs, gebruikmakend van het voorgaande resultaat, dat er oneindig veel priemgetallen p van de vorm $p \equiv 1 \pmod 5$ zijn.

4. Neem aan dat het *abc*-vermoeden geldt. Zij A, B een tweetal gegeven positieve gehele getallen. Bewijs dat er hooguit eindig veel positieve gehele getallen x, y zijn zó dat

$$Ax^2 - By^3 = 1.$$

5. Bewijs dat
$$\sum_{n=1}^{\infty} \frac{1}{q^n (n!)^2}$$
irrationaal is voor elke $q \in \mathbb{N}$.

UITWERKINGEN

1. First solve $37x \equiv 4 \pmod{85}$. Multiplication with the inverse of 37 (mod 85) gives us $x \equiv 7 \pmod{85}$. The equation $x^2 \equiv 9 \pmod{100}$ is equivalent to the simultaneous equations
$$x^2 \equiv 1 \pmod{4}, \qquad x^2 \equiv 9 \pmod{25}.$$
The first is equivalent to $x \equiv 1 \pmod{2}$ and the second implies $25|x^2-9$ hence $25|(x-3)(x+3)$. Since $x+3$ and $x-3$ cannot be both divisible by 5 we conclude that $x \equiv \pm 3 \pmod{25}$. We now solve the following systems
$$x \equiv 7 \pmod{85} \quad x \equiv 1 \pmod{2} \quad x \equiv 3 \pmod{25}$$
and
$$x \equiv 7 \pmod{85} \quad x \equiv 1 \pmod{2} \quad x \equiv -3 \pmod{25}$$
The first system has no solutions since the first equation implies $x \equiv 2 \pmod{5}$ and the third $x \equiv 3 \pmod{5}$. Standard solution of the second equation yields $x \equiv 347 \pmod{850}$.

2. (a) Suppose p is odd. Then
$$\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) = (-1)^{(p-1)/2} \cdot (-1)^{(p-1)/2} \left(\frac{p}{3}\right)$$
where the last equality is an application of quadratic reciprocity. Since p is odd we have $(-1)^{(p-1)/2} \cdot (-1)^{(p-1)/2} = 1$ and since $\left(\frac{p}{3}\right)$ is 1 if and only if $p \equiv 1 \pmod{3}$ we find that -3 is a quadratic residue modulo p if and only if $p \equiv 1 \pmod{3}$. The cases $p = 2, 3$ can be considered separately.

   (b) The order of -3 modulo q is a divisor of $q - 1 = 2p$. Hence the possible orders are $1, 2, p, 2p$. In the last case -3 is a primitive root modulo q. We now check the smaller orders.
   $(-3)^1 \equiv 1 \pmod{q}$ implies $q|4$ which is impossible since $q > 7$.
   $(-3)^2 \equiv 1 \pmod{q}$ implies $q|7$ which is again excluded.

$(-3)^p \equiv 1 \pmod q$ implies $\left(\frac{-3}{q}\right) = 1$ because $(-3)^p = (-3)^{(q-1)/2}$ and Euler's theorem. From part (a) we know that $q \equiv 1 \pmod 3$ and hence $2p+1 \equiv 1 \pmod 3$. This implies $p \equiv 0 \pmod 3$ so p cannot be prime. We get a contradiction.
We conclude that $-3 \pmod q$ has order $q-1$.

3. (a) When p is a prime divisor of $x^4+x^3+x^2+x+1$ it also divides x^5-1. Hence $x^5 \equiv 1 \pmod p$. The order of $x \pmod p$ is 1 or 5. Suppose it is 1. Then $x \equiv 1 \pmod p$ and from $x^4+x^3+x^2+x+1 \equiv 0 \pmod p$ it follows that $5 \equiv 0 \pmod p$. Hence p divides 5, so $p = 5$. When the order is 5 we note that the order divides $p-1$, hence $p \equiv 1 \pmod 5$.

   (b) Suppose there are finitely many primes $p_1, \dots, p_r$ which are $1 \pmod 5$. Let $N = 5p_1 \cdots p_r$ and consider the number $N^4+N^3+N^2+N+1$. Let q be any prime divisor of this number. By construction it cannot be equal to 5 or $1 \pmod 5$. By the previous result we know it should be of this form. So we have a contradiction. There are infinitely many primes of the form $1 \pmod 5$.

4. Notice that $Ax^2 = 1 + By^3$ and $\gcd(Ax^2, By^3, 1) = 1$. So we can apply the abc-conjecture with $a = 1, b = By^3, c = Ax^2$. We get for any $\epsilon > 0$ a positive number $c(\epsilon)$ such that

$$\begin{aligned} Ax^2 &< c(\epsilon)(\mathrm{rad}(ABx^2y^3))^{1+\epsilon} \\ &= c(\epsilon)(\mathrm{rad}(ABxy))^{1+\epsilon} \\ &\leq c(\epsilon)(ABxy))^{1+\epsilon} \end{aligned}$$

   We now use that $y^3 < Ax^2/B \leq Ax^2$. Hence $y < Ax^{2/3}$ and so

$$Ax^2 < c(\epsilon)(A^2Bx^{5/3}))^{1+\epsilon}$$

   Now choose $\epsilon = 1/10$. Then $Ax^{2-5.5/3} < c(0.1)(A^2B)^{1.1}$. Since $2 - 5.5/3 = 1/6 > 0$ we see that x is bounded. Hence there are finitely many possibilities for x and by $By^3 = Ax^2 - 1$ the same holds for y.

5. Suppose the number is rational, say a/b. Choose $k > 1$ and consider the difference

$$\delta = \frac{a}{b} - \sum_{n=1}^{k} \frac{1}{q^n (n!)^2}.$$

   Note that this is a rational number whose denominator divides $bq^n(n!)^2$. Hence, since $\delta > 0$,

$$\delta \geq \frac{1}{bq^n(n!)^2}.$$

On the other hand the difference equals

$$\begin{aligned}
\delta &= \sum_{n=k+1}^{\infty} \frac{1}{q^n (n!)^2} \\
&= \frac{1}{q^{k+1}((k+1)!)^2} + \frac{1}{q^{k+2}((k+2)!)^2} + \frac{1}{q^{k+3}((k+3)!)^2} + \cdots \\
&\leq \frac{1}{q^k} \left(\frac{1}{((k+1)!)^2} + \frac{1}{((k+2)!)^2} + \frac{1}{((k+3)!)^2} + \cdots \right) \\
&< \frac{1}{q^k((k+1)!)^2} \left(1 + \frac{1}{k^2} + \frac{1}{k^4} + \cdots \right)
\end{aligned}$$

The last sum can be estimated by $1 + 1/2 + 1/2^2 + \cdots = 2$ and we get

$$\delta < \frac{2}{q^k((k+1)!)^2}.$$

This contradicts the lower bound as soon as $(k+1)^2 > 2b$.