Solutions for Number theory, Talteori 6hp, Kurskod TATA54, Provkod TEN1
June 4, 2020
LINKÖPINGS UNIVERSITET
Matematiska Institutionen
Examinator: Jan Snellman

1) Find all integers n such that $n+1$ is *not* divisible by 3 and $n+2$ is divisible by 5.

   Solution: Clearly, $n+1$ is indivisible by 3 iff $n \equiv 0, 1 \mod 3$, and $n+2$ is divisible by 5 iff $n \equiv 3 \mod 5$. By the Chinese remainder theorem, the case $n \equiv 0 \mod 3$ and simultaneously $n \equiv 3 \mod 5$ is equivalent to $n \equiv 3 \mod 15$. Similarly, $n \equiv 1 \mod 3$ and simultaneously $n \equiv 3 \mod 5$ iff $n \equiv 13 \mod 15$. In conclusion, $n \equiv 3, 13 \mod 15$.

2) Let n be a positive integer. How many solutions are there to the congruence $x^3 + x \equiv 0 \mod 2^n$?

   Solution: Modulo 2, both 0 and 1 are roots, but modulo 4 only 0 is a root. The formal derivative is $3x^2 + 1$, which evaluates to 1 at zero, so this zero will lift uniquely henceforth.

3) How many primitive roots are there mod 7? Find them all. For each primitive root a mod 7 that you find, check which of the "lifts"

$$a + 7t, \qquad 0 \leq t \leq 6$$

   are primitive roots mod 49.

   Solution: We see that 2 is not a primitive root modulo 7, but 3 is. Since $\phi(7) = 6$, the primitive roots modulo 7 are 3^1 and $3^5 \equiv 5 \mod 7$.

   A dumb search reveals that all lifts of 3 except $31 = 3 + 4 * 7$ are primitive roots modulo 49, as are all lifts of 5 except $19 = 5 + 2 * 7$.

4) Determine the (periodic) continued fraction expansion of $\sqrt{3}$ by finding the minimal algebraic relation satisfied by $\sqrt{3} - 1$.

   Solution: Put $a = \sqrt{3} - 1$, $a^* = -\sqrt{3} - 1$. Then a, a^* are the zeroes of $(x-a)(x-a^*) = x^2 + 2x - 2$. So $a(3+a) = 2+a$, hence $a = (2+a)/(3+a)$. It follows that

$$a = \frac{1}{1 + \frac{1}{2+a}} = [0; \overline{1, 2}]$$

   whence $\sqrt{3} = a + 1 = [1; \overline{1, 2}]$.

5) For a positive integer n, let $[n] = \{1, 2, \ldots, n\}$, $[n]^2 = \{\, (i,j) | i, j \in [n] \,\}$, $C(n) = \left\{\, (i,j) \in [n]^2 \middle| \gcd(i,j) = 1 \,\right\}$. Show that

$$\#C(n) = \sum_{d=1}^{n} \mu(d) \lfloor \frac{n}{d} \rfloor^2.$$

Solution: For any predicate P, we say that $[P] = 1$ if P is true, and zero otherwise. With this notation,

$$\#C(n) = \sum_{i=1}^{n}\sum_{j=1}^{n}[\gcd(i,j) = 1].$$

By Möbius inversion, $[n = 1] = \sum_{d\,|\,n} \mu(d)$, and in particular

$$[\gcd(i,j) = 1] = \sum_{d\,|\,\gcd(i,j)} \mu(d).$$

Hence

$$\begin{aligned}
\#C(n) &= \sum_{i=1}^{n}\sum_{j=1}^{n}[\gcd(i,j) = 1] \\
&= \sum_{i=1}^{n}\sum_{j=1}^{n}\sum_{d\,|\,\gcd(i,j)} \mu(d) \\
&= \sum_{i=1}^{n}\sum_{j=1}^{n}\sum_{d=1}^{n}[d\,|\,\gcd(i,j)]\mu(d) \\
&= \sum_{i=1}^{n}\sum_{j=1}^{n}\sum_{d=1}^{n}[d\,|\,i][d\,|\,j]\mu(d) \\
&= \left(\sum_{d=1}^{n}\mu(d)\right)\left(\sum_{i=1}^{n}[d\,|\,i]\right)\left(\sum_{j=1}^{n}[d\,|\,j]\right) \\
&= \sum_{d=1}^{n}\mu(d)\lfloor\frac{n}{d}\rfloor^2
\end{aligned}$$

where we have used that $[d\,|\,\gcd(i,j)] = [d\,|\,i][d\,|\,j]$ and that $\sum_{i=1}^{n}[d\,|\,i] = \lfloor\frac{n}{d}\rfloor$.