Number theory, Talteori 6hp, Kurskod TATA54, Provkod TEN1
August 26, 2017
LINKÖPINGS UNIVERSITET
Matematiska Institutionen
Examinator: Jan Snellman

Each problem is worth 3 points. To receive full points, a solution needs to be complete. Indicate which theorems from the textbook that you have used, and include all auxillary calculations.

No aids, no calculators, tables, nor texbooks.

1) Find all integers x such that

$$\begin{aligned} x &\equiv 5 \mod 11 \\ 2x &\equiv 1 \mod 13. \end{aligned}$$

2) How many incongruent solutions are there to the congruence

$$5x^3 + x^2 + x + 1 \equiv 0 \mod 32?$$

3) Use the fact that 3 is a primitive root modulo 17 to find all solutions to the congruence

$$10^x \equiv 5 \mod 17.$$

4) Let $x = [1; \overline{1, 2}]$. Compute the value of x.

5) Let $p > 3$ be a prime. Show that

$$\left(\frac{3}{p}\right) = 1 \qquad \iff \qquad p \equiv \pm 1 \mod 12$$

6) Let $\omega(n)$ be the number of distinct primes that divide n, $\tau(d)$ be the number of positive divisors of d, and let μ be the Möbius function.

(a) Show that $n \mapsto 3^{\omega(n)}$ is multiplicative.

(b) Using the above, and the fact that τ and μ are multiplicative, show that

$$\sum_{d|n} |\mu(d)| \tau(d) = 3^{\omega(n)}$$

Solutions to Number theory, Talteori 6hp, Kurskod TATA54, Provkod TEN1
August 26, 2017

1) Find all integers x such that

$$x \equiv 5 \mod 11$$
$$2x \equiv 1 \mod 13.$$

Solution: Since 7 is the inverse of 2 mod 13, this is equivalent to

$$x \equiv 5 \mod 11$$
$$x \equiv 7 \mod 13.$$

This gives that

$$x = 5+11s \equiv 7 \mod 13 \implies 11s \equiv 2 \mod 13 \implies s \equiv -1 \mod 13$$

so $x \equiv -6 \mod 13 * 11$.

2) How many incongruent solutions are there to the congruence

$$5x^3 + x^2 + x + 1 \equiv 0 \mod 32?$$

Solution: $f(x) = 5x^3 + x^2 + x + 1$ has the unique zero $r = 1$ mod 2. We have that $f'(x) = 15x^2 + 2x + 1$, $f'(r) = 0 \mod 2$, and $f(r) = 0 \mod 4$, so both lifts of r, namely 1 and 3, are zeroes mod 4.

We continue to lift the zeroes to higher powers of two. Note that for each s such that $f(s) = 0 \mod 2^{k-1}$, if s is odd then $f'(s) = 0 \mod 2$, hence either $f(s) = 0 \mod 2^k$, in which case Hensel's lemma guarantees that $s + 2^{k-1}$ is also a zero mod 2^k, or $f(s) \neq 0 \mod 2^k$, in which $s + 2^{k-1}$ is not a zero mod 2^k, either.

We get: the lifts of $1 \mod 4$ are $1 \mod 8$ and $5 \mod 8$, they are zeroes of f. The lifts of $3 \mod 4$ are not zeroes of f mod 4.

The lifts of $1 \mod 8$ are not zeroes. The lifts of $5 \mod 8$ are $5 \mod 16$ and $13 \mod 16$, they are zeroes.

The lifts of $5 \mod 16$ are not zeroes. The lifts of $13 \mod 16$ are 13 mod 32 and $29 \mod 32$, they are zeroes of f.

Thus there are two incogruent solutions mod 32.

3) Use the fact that 3 is a primitive root modulo 17 to find all solutions to the congruence

$$10^x \equiv 5 \mod 17.$$

Solution: Taking indices w.r.t. the primitive root 3, the equation becomes

$$x\text{ind}(10) \equiv \text{ind}(5) \mod 16,$$

or

$$3x \equiv 5 \mod 16,$$

hence $x \equiv 7 \mod 16$.

4) Let $x = [1; \overline{1, 2}]$. Compute the value of x.

Solution: Let $y = x - 1$, then

$$y = \frac{1}{1 + \frac{1}{2+y}} = \frac{2+y}{3+y}$$

which has the positive root $\sqrt{3} - 1$. Hence $x = \sqrt{3}$.

5) Let $p > 3$ be a prime. Show that

$$\left(\frac{3}{p}\right) = 1 \quad \Longleftrightarrow \quad p \equiv \pm 1 \mod 12$$

Solution: : This is exercise 11.2.2 in Rosen.

6) Let $\omega(n)$ be the number of distinct primes that divide n, $\tau(d)$ be the number of positive divisors of d, and let μ be the Möbius function.

(a) Show that $n \mapsto 3^{\omega(n)}$ is multiplicative.

(b) Using the above, and the fact that τ and μ are multiplicative, show that

$$\sum_{d|n} |\mu(d)|\tau(d) = 3^{\omega(n)}$$

Solution: : This exercise was given in the exam on August 23, 2012.