Number theory, Talteori 6hp, Kurskod TATA54, Provkod TEN1
June 7, 2018
LINKÖPINGS UNIVERSITET
Matematiska Institutionen
Examinator: Jan Snellman

Solutions.

1) Determine all solutions to the congruence

$$f(x) \equiv 0 \mod 2^k$$

for $1 \leq k \leq 3$, when

(a) $f(x) = x^2 + x$,
(b) $f(x) = 2x^2$.

Solution: In case (a), both 0 and 1 are solutions modulo 2. We have that

$$f'(x) = 2x + 1 \equiv 1 \mod 2,$$

so both solutions lift uniquely to a solution mod 4. Clearly, 0 lifts to 0, and we check that the lift $3 = 1 + 1 * 2$ is a solution mod 4 (whereas $1 = 1 + 0 * 2$ is not). Similarly, the solution $x \equiv 0 \mod 4$ lifts to $x \equiv 0 \mod 8$, and $x \equiv 3 \mod 4$ lifts to $x \equiv 7 \mod 8$.

In case (b), both 0 and 1 are again solutions mod 2. We have that $f'(x) = 4x \equiv 0 \mod 2$, so the solutions mod 2 will not lift uniquely to solutions mod 4; rather, they either lift in all possible ways or do not lift at all.

Since $x = 0$ is a zero of f mod 4, it follows that $x = 2$ is as well. However, $x = 1$ is not a zero mod 4, so neither is $x = 3$. Thus the solutions mod 4 is $x \equiv 0 \mod 4$ together with $x \equiv 2 \mod 4$.

Since $f(0) = 0$, $f(2) = 8$ are both zero mod 8, we get that both these zeroes mod 4 lift in all possible ways to yield zeroes mod 8; these are therefore

$$x \equiv 0, 2, 4, 6 \mod 8.$$

2) Calculate

$$\alpha = 1 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{1 + \dots}}}}$$

Solution: Since

$$\alpha = 1 + \frac{1}{2 + \frac{1}{\alpha}}$$

we get that

$$\alpha - 1 = \frac{1}{2 + 1/\alpha} = \frac{\alpha}{2\alpha + 1}$$

so that α is the positive root of

$$(\alpha - 1)(2\alpha + 1) = \alpha,$$

which is $\alpha = \frac{1}{2} + \frac{\sqrt{3}}{2}$.

3) Let $n = 20000128$. Determine the positive integer k such that 2^k divides n but 2^{k+1} does not divide n.

   Solution: Note that

$$n = 2 * 10^7 + 2^7 = 2^8 * 5^7 + 2^7.$$

   We see that n is divisible by 2^7 but not 2^8.

4) Show that all sufficiently large integers can be expressed as a non-negative integer combination of 9 and 11, and determine the largest integer that can not be so expressed.

   Solution: Since $\gcd(9, 11) = 1 = 9 * 5 + 11 * (-4)$, the Diophantine equation

$$9x + 11y = d$$

   is solvable for all d. However, it is not necessarily solvable in non-negative integers; for instance, if $1 \leq d \leq 8$ there is no solution with non-begative integers.

   The general solution (in integers) is

$$(x, y) = (5d, -4d) + t(-11, 9), \qquad t \in \boldsymbol{Z}.$$

   If $x, y \geq 0$, then

$$5d - 11t \geq 0, \quad -4d + 9t \geq 0,$$

   or equivalently,

$$44d \leq 99t \leq 45d.$$

   We see that once $d \geq 99$ there is certainly at least one positive integer t which works. This proves the first part.

   For the second part, we put, for $0 \leq j \leq 8$,

$$r_j = 11j,$$

   so

$$r_0 = 0,\ r_1 = 11,\ r_2 = 22,\ r_3 = 33,\ r_4 = 44,\ r_5 = 55,\ r_6 = 66,\ r_7 = 77,\ r_8 = 88.$$

Then, since 9 and 11 are relatively prime, all r_j are non-congruent modulo 9, and thus constitute a complete set of residues modulo 9. All r_j are of course non-negative integer combinations of 9 and 11, and so is $r_j + 9k$ for all integers $k \geq 0$. We get that all integers $\geq r_8$ can be expressed as a non-negative integer combination of 9 and 11.

On the other hand, $r_j - 9 = 9 * (-1) + 11 * j$ is not a non-negative integer combination of 9 and 11, since you get a new solution by adding $s(11, -9)$ to an old solution, and $0 \leq j \leq 8$.

We conclude that the largest integer d which can not be expressed as a non-negative integer combination of 9 and 11 is

$$r_8 - 9 = 88 - 9 = 79.$$

5) For which primes p is the congruence

$$x^2 \equiv 5 \mod p$$

solvable?

Solution: For odd $p \neq 5$, the congruence is solvable if and only if

$$\left(\frac{5}{p}\right) = 1.$$

Since $5 \equiv 1 \mod 4$, quadratic reciprocity gives that cdis

$$\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right).$$

Since

$$0^2 \equiv 0,\ 1^2 \equiv 1,\ 2^2 \equiv 4,\ 3^2 \equiv 4,\ 4^2 \equiv 1 \mod 5$$

the quadratic residues mod 5 are $1, 4$, thus we should have

$$p \equiv 1, 4 \mod 5$$

for the original congruence to be solvable.

When $p = 2$, we check that $5^2 \equiv 5 \mod 2$, so the congruence is solvable also in this case.

When $p = 5$, $5^2 \equiv 5 \mod 2$, so the congruence is solvable also in this case.

6) Find a positive integer a which is a primitive root modulo 5^k for all integers $k \geq 1$.

Solution: : Since $a = 2$ has order 4 modulo 5, it is a primitive root modulo 5. The maximal order of an integer modulo 25 is $\phi(5^2) = 5^2 - 5 = 20 = 2 * 2 * 5$. We check that $2^2, 2^4, 2^{10}$ are all non-congruent to 1 mod 25, so $a = 2$ has order 20 and is a primitive root, modul0 25.

Since $a = 2$ is a primitive root modulo 5 and modulo 5^2, it is a primitive root modulo 5^k for all positive k, by a theorem in the textbook.