ELEMENTARY NUMBER THEORY AND CRYPTOGRAPHY II
SOLUTIONS FOR PROBLEM SHEET 3
EPIPHANY TERM 2015

(1) We consider the cases,

If $n = 2m$ is even then $2^n = (2^m)^2 + 0^2$.

If $n = 2m + 1$ is odd then $2^n = (2^m)^2 + (2^m)^2$.

(2) Suppose $n = a(a+1)/2 + b(b+1)/2$ with $a, b \in \mathbb{Z}$. Then $4n+1 = 2a(a+1) + 2b(b+1)+1 = (a^2-2ab+b^2)+(a^2+b^2+2ab+2a+2b+1) = (a-b)^2+(a+b+1)^2$.

(3) Suppose $n = a^2 + b^2$ is the sum of two square with $a, b \in \mathbb{Z}$. Note that a^2 or b^2 can be congruent only to 0 or 1 modulo 4. Therefore, n can be congruent only to 0,1 or 2 and can't be congruent to 3 modulo 4. But one of four consecutive integers will be always congruent to 3 modulo 4 and therefore can't be written as a sum of two squares.

(4) Suppose $p = p_1^2 + p_2^2 + p_3^2$, where p, p_1, p_2, p_3 are primes. If neither of p_1, p_2, p_3 equals three then $p_1^2 \equiv p_2^2 \equiv p_3^2 \equiv 1 \bmod 3$ and p is divisible by 3, but $p \geqslant 2^2 + 2^2 + 2^2 = 12$.

(5) Note that $b \not\equiv 0 \bmod p$ (otherwise $a \equiv 0 \bmod p$ and $\gcd(a, b) \neq 1$). Then $a^2 + b^2 \equiv 0 \bmod p$ implies that $(a/b)^2 \equiv -1 \bmod p$. So -1 is a quadratic residue modulo p and $p \equiv 1 \bmod 4$. Therefore, all prime divisors of $a^2 + b^2$ are congruent to 1 modulo 4. This implies that any divisor of $a^2 + b^2$ satisfies the same condition and is therefore a sum of two squares.

(6) If $p = 8k + 1$ then both -1 and 2 are quadratic residues modulo p. If $p = 8k + 3$ then both -1 and 2 are not quadratic residues modulo p. Therefore, in both above cases -2 is a quadratic residue modulo p. Now mimic the proof of Theorem that $p = a^2+b^2$ if $p \equiv 1 \bmod 4$ (or equivalently, if -1 is a quadratic residue modulo p).

Let $\alpha \in \mathbb{Z}$ be such that α^2 is congruent to -2 modulo p. Then $x^2 + 2y^2 \equiv (x - \alpha y)(x + \alpha y) \bmod p$.

Consider the set $S = \{(x_0, y_0) \mid 0 \leqslant x_0, y_0 < \sqrt{p}\}$.

Then S contains more than $\sqrt{p} \cdot \sqrt{p} = p$ elements and there are two different elements $(x_1, y_1), (x_2, y_2) \in S$ such that

$$x_1 - \alpha y_1 \equiv x_2 - \alpha y_2 \bmod p.$$

Therefore, for $x_0 = x_1 - x_2$ and $y_0 = y_1 - y_2$, we have $-\sqrt{p} < x_0, y_0 < \sqrt{p}$, $(x_0, y_0) \neq (0, 0)$, and $x_0^2 + 2y_0^2 \equiv (x_0 - \alpha y_0)(x_0 + \alpha y_0) \equiv 0 \bmod p$.

But this means that $0 < x_0^2 + 2y_0^2 < 3p$ and, therefore, $x_0^2 + 2y_0^2$ equals to either p or $2p$. In the first case our problem is solved. In the second case x_0 is divisible by 2 and substituting $x_0 = 2x_1$ we obtain $y_0^2 + 2x_1^2 = p$.

(7) We note that

$$2^{2n+1} = (2^{2n-k} + 2^{k-1})^2 - (2^{2n-k} - 2^{k-1})^2$$

Hence for any given n, and for $k = 1, \ldots, n$ we get n different ways to write the integer 2^{2n+1} as the difference of two squares.

(8) Since n cannot be written as the sum of two squares then by the theorem in the lectures there exist a prime p, with $p \equiv 3 \pmod 4$ such that $p^k | n$ and $p^{k+1} \not| n$ for some odd k. If n could be written as the sum of two squares of two rational numbers then we would have

$$n = \left(\frac{a}{b}\right)^2 + \left(\frac{c}{d}\right)^2$$

with $a, b, c, d \in \mathbb{Z}$. This is equivalent to

$$n(bd)^2 = (ad)^2 + (bc)^2$$

However when we consider the prime factorization of the above numbers, in the left hand side of the above equation the prime p appears in an odd power. However in the right hand side, since the number is the sum of two squares, has to appear in an even power. Contradiction

(9) Let r be an odd primitive root modulo p. (why does it always exist?) Then for some integer $k > 1$ we have

$$r^k \equiv 2 \pmod p$$

or $r^{2k} \equiv 4 \pmod p$. Moreover we have $r^{\frac{p-1}{2}} \equiv -1 \pmod p$. So together

$$r^{2k+\frac{p-1}{2}} + 4 \equiv 0 \pmod p$$

Since $p \equiv 1 \pmod p$ we can rewrite

$$r^{2(k+\frac{p-1}{4}} + 2^2 \equiv 0 \pmod p$$

or

$$\left(r^{k+\frac{p-1}{4}}\right)^2 + 2^2 \equiv 0 \pmod p$$

So p divides the sum of two squares $\left(r^{k+\frac{p-1}{4}}\right)^2 + 2^2$ which are relative prime since $gcd(r, 2) = 1$, and clearly both exceed 3.

(10) We rewrite the equation as

$$x^2 + y^2 + z^2 + x + y + z = 1.$$

We multiply by 4 and get

$$(2x)^2 + (2y)^2 + (2z)^2 + 4x + 4y + 4z = 4$$

and by adding 3 to both sides

$$(2x)^2 + 4x + 1 + (2y)^2 + 4y + 1 + (2z)^2 + 4z + 1 = 7$$

or

$$(2x + 1)^2 + (2y + 1)^2 + (2z + 1)^2 = 7.$$

In particular if there exist x,y,z which solve the original equation then we could write 7 as the sum of three cubes, which we know it is not possible.

(11) If $p = a^3 + b^3$ with $a, b \in \mathbb{N}$ then $p = (a+b)(a^2 - ab + b^2)$ implies that $a + b = p$ and $a^2 - ab + b^2 = 1$. But the second condition gives $(a - b)^2 + ab = 1$, $ab \leqslant 1$ and therefore $a = b = 1$.

(12) (a) 187=**3** 57+16; 57=**3** 16+9; 16=**1** 9+7;
9=**1** 7+2; 7=**3** 2+1; 2=**2**+0. Therefore, $187/57 = [3; 3, 1, 1, 3, 2]$.

(b) 71=**1** 55+16; 55=**3** 16+7; 16=**2** 7+2;
7=**3** 2+1; 2=**2**+0. Therefore, $71/55 = [1; 3, 2, 3, 2]$.

(c) 118/303=**0** 303+118/303; 303/118=**2** 118+67/118; 118=**1** 67+51; 67=**1** 51+16; 51=**3** 16+3; 16=**5** 3+1; 3=**3**+0. Therefore, $118/303 = [0; 2, 1, 1, 3, 5, 3]$.

(13) Use the relations $p_0 = a_0$, $q_0 = 1$, $p_1 = a_0 a_1 + 1$, $q_1 = a_1$ and for $k \geqslant 2$, $p_k = a_k p_{k-1} + p_{k-2}$ and $q_k = a_k q_{k-1} + q_{k-2}$:

a)

a_k :	-2	2	4	6	8
p_k :	-2	-3	-14	-87	-710
q_k :	1	2	9	56	457

and the number equals the last convergent $p_5/q_5 = -710/457$.

b)

a_k :	4	2	1	3	1	2	4
p_k :	4	9	13	48	61	170	741
q_k :	1	2	3	11	14	39	170

and the number equals the last convergent $p_6/q_6 = 741/170$.

c)

a_k :	0	1	2	3	4	3	2	1
p_k :	0	1	2	7	30	97	224	321
q_k :	1	1	3	10	43	139	321	460

and the number equals the last convergent $p_7/q_7 = 321/460$.

(14) Use that $q_0 = 1$ and for $k \geqslant 2$, $q_k = a_k q_{k-1} + q_{k-2} \geqslant 2q_{k-2}$ to obtain $q_{2n} \geqslant 2^n$ for all $n \in \mathbb{N}$. For odd indices use that $q_{2n-1} \geqslant q_{2n-2}$.

(15) (a) Let $\overline{[2;3]}$. Then the relation $x = 2 + \cfrac{1}{3 + \cfrac{1}{x}}$ implies that $x = 1 + \sqrt{15}/3$.

(b) Let $x = \overline{[1;2,3]}$. Then $x = 1 + \cfrac{1}{2 + \cfrac{1}{3 + \cfrac{1}{x}}}$ implies that

a_k :	1	2	3	x
p_k :	1	3	10	$10x + 3$
q_k :	1	2	7	$7x + 2$

Therefore, $x = (10x+3)/(7x+2)$ gives $7x^2 - 8x - 3 = 0$, $x = (4+\sqrt{37})/7$ and $x^{-1} = [0; \overline{1,2,3}] = (\sqrt{37} - 4)/3$.