NUMBER THEORY, TATASY, August 31, 2013

① First factorize 9996 into prime numbers:

$9996 = 10000 - 4 = 100^2 - 2^2 = 102 \cdot 98 =$
$= 2^2 \cdot 3 \cdot 7^2 \cdot 17$. There is a prime $\equiv 3 \pmod 4$ (namely 3) which occurs to an odd power. Therefore there are no integers x, y such that $x^2 + y^2 = 9996$.

<u>ANSWER</u>: No solutions

② Each prime $p \leq 100$ divides $100!$ and therefore not N. But 101 is a prime number, and by Wilson's theorem $101 \mid N$. <u>ANSWER</u>: 101

③ Let $f(x) = x^2 - 2x - 1$

(a) $x^2 - 2x - 1 \equiv 0 \pmod 7 \iff$
$(x-1)^2 - 2 \equiv 0 \pmod 7 \iff$
$(x-1)^2 - 3^2 \equiv 0 \pmod 7 \iff$
$\equiv 0 \pmod 7 \iff (x-1-3)(x-1+3)$
$\iff (x-4)(x+2) \equiv 0 \pmod 7$
$\iff x - 4 \equiv 0 \pmod 7$ or $x + 2 \equiv 0 \pmod 7$
$\iff x \equiv 4$ or $5 \pmod 7$

(b) $f'(x) = 2x - 2$
Since $f'(4) = 6$ and $f'(5) = 8$ are not divisible by 7, we know by Hensel's lemma that the solutions of $f(x) \equiv 0 \pmod 7$ can be uniquely be lifted to solutions of $f(x) \equiv 0 \pmod{7^2}$

• $f(4+7t) = (4+7t)^2 - 2(4+7t) - 1 =$
$= \cancel{16} + 8 \cdot 7t + 7^2t^2 - 8 - 2 \cdot 7t - 1 =$
$= 7 + 6 \cdot 7t + 7^2t^2 \equiv 7(1+6t) \pmod{7^2}$
$f(4+7t) \equiv 0 \pmod{7^2} \iff 1 + 6t \equiv 0 \pmod 7$
$\iff 1 - t \equiv 0 \pmod 7 \iff t \equiv 1 \pmod 7$
i.e. $t = 1 + 7n, n \in \mathbb{Z}$

(3b Ctd) The solutions of $f(x) \equiv 0 \pmod{7^2}$ which are $\equiv 4 \pmod 7$ are

$x = 4 + (1+7n)7 = 11 + 7^2 \cdot n$, $n \in \mathbb{Z}$

Similarly $f(\cancel{5}+7t) \equiv 7(9+8t) \bmod 7^2$

So $f(5+7t) \equiv 0 \pmod{7^2} \iff$

$9+8t \equiv 0 \pmod 7 \iff \cancel{9} \, 2+t \equiv 0 \pmod 7 \iff t \equiv 5 \bmod 7$

Soln of $f(x) \equiv 0 \pmod{7^2}$ (congruent to 5 mod 7) are $X = 5 + 7(5+7n) =$

$= 40 + 7^2 n$, $n \in \mathbb{Z}$

Answer: (a) $x \equiv 4$ or $5 \pmod 7$

(b) ~~All the~~ numbers of the form

$x = 11 + 49n$, $n \in \mathbb{Z}$ or

$x \equiv 40 + 49n$, $n \in \mathbb{Z}$

(4) (a) By using the algorithm $\alpha_0 = \sqrt{12}$, $a_n = [\alpha_n]$, $\alpha_{n+1} = \dfrac{1}{\alpha_n - a_n}$

One easily gets

$\sqrt{12} = [3; \overline{2,6}]$

(b) Compute convergents $C_k = \frac{p_k}{q_k}$, $C_0 = 3$, $C_1 = 3 + \frac{1}{2} = \frac{7}{2}$

$C_2 = 3 + \dfrac{1}{2+\frac{1}{6}} = \dfrac{45}{13}$.

By the ~~formula~~ inequality $|\sqrt{12} - C_k| < \frac{1}{q_k^2}$, we get $\left|\sqrt{12} - \frac{45}{13}\right| < \frac{1}{13^2} < \frac{1}{100}$

ANSWER: (a) $\sqrt{12} = [3; \overline{2,6}]$

(b) $\frac{45}{13}$

5.(a) $\operatorname{ord}_{31} 3 \mid 30$

$3^3 = 27 \equiv -4 \pmod{31}$, $3^4 = 3 \cdot 3^3 \equiv 3(-4) \equiv -$ (mod 3

$3^5 \equiv 3(-12) \equiv -36 \equiv -5 \pmod{31}$

$3^6 \equiv (3^3)^2 \equiv 16 \pmod{31}$

$3^{10} = (3^5)^2 \equiv 25 \equiv -6 \pmod{31}$

$3^{15} = 3^5 \cdot 3^{10} \equiv (-5)(-6) \equiv 30 \equiv -1$ (m

Hence $\operatorname{ord}_{31} 3 = 30$, i.e. 3 is a primitive

(b) Use index arithmetic with the primitive root found in (a):

$5x^7 \equiv 3 \pmod{31} \iff \operatorname{ind}_3(5x^7) \equiv \operatorname{ind}_3 3$ (mod

$\iff \operatorname{ind}_3 5 + 7 \operatorname{ind}_3 x \equiv 1 \pmod{30}$

$3^{20} = 3^5 \cdot 3^{15} \equiv (-5)(-1) \equiv 5 \pmod{30}$ $\iff$

$\iff 20 + 7 \operatorname{ind}_3 x \equiv 1 \pmod{30}$

$\iff$

$7 \operatorname{ind}_3 x \equiv 11 \pmod{30}$

$\iff$ / $(7,30)=1$ /

$7 \cdot 7 \operatorname{ind}_3 x \equiv 7 \cdot 11 \pmod{30} \equiv$

$\equiv -11 \operatorname{ind}_3 x \equiv 7 \cdot 11 \pmod{30}$

$\iff$ $(11,30)=1$ $-\operatorname{ind}_3 x \equiv \cancel{77} \pmod{30} \iff$

$\operatorname{ind}_3 x \equiv -7 \equiv 23 \pmod{30}$.

$x \equiv 3^{23} \equiv 3^{20} \cdot 3^3 \equiv 5 \cdot (-4) \equiv$

$\equiv -20 \equiv 11 \pmod{31}$

ANSWER: (a) e.g. 3

(b) $x \equiv 11 \pmod{31}$

(6) (a) 61 is a prime number and therefore has a primitive root.

$\mathrm{ord}_{61} 2 \nmid 60 = 2^2 \cdot 3 \cdot 5$

$2^6 = 64 \equiv 3 \pmod{61}$

$2^{10} = 2^4 \cdot 2^6 \equiv 48$ ~~mod~~ $-13 \pmod{61}$

$2^{12} = (2^6)^2 \equiv 9 \pmod{61}$

$2^{15} \equiv 2^{12} \cdot 2^3 \equiv 9 \cdot 8 \equiv 11 \pmod{61}$

$2^{20} \equiv (2^6)^3 \cancel{2}^2$ ~~$16\,2$~~ $\equiv 27 \cdot 4 \equiv$

$\equiv 54 \cdot 2 \equiv (-7)2 \equiv -14 \pmod{61}$

$2^{30} \equiv (2^{15})^2 \equiv 121 \equiv -1 \pmod{61}$

(b) $7442 = 2 \cdot 61^2$ and 61 is a prime number so 7442 has a prim root.

We first show that 2 ~~has the~~ is the prim root of 61^2

We need only show that $2^{60} \not\equiv 1 \pmod{61^2}$

$2^6 = 3 + 61$, $2^{30} = (3+61)^5 \equiv$

$\equiv 3^5 + 5 \cdot 3^4 \cdot 61 \equiv 3^4(3 + 5 \cdot 61) \equiv$

$\equiv (20+61)(3+5 \cdot 61) \equiv 60 + 103 \cdot 61$

$\equiv -1 + 61 + 103 \cdot 61 \equiv -1 + (42+61) \cdot 61 \equiv -1 + 42 \cdot 61$

~~$\equiv -1 + 61 + 3 \cdot 61$~~

$\not\equiv 1 \pmod{61^2}$

Since 2 is a prim root mod 61^2,

$2 + 61^2 = 2 + 3721 = 3723$ is a prim root of $2 \cdot 61^2$.

ANSWER: (a) eg 2

(b) e.g. 3723