Ex sheet 3

Ex 1: 1. $(\mathbb{Z}/15\mathbb{Z})^\times = \{1, 2, 4, 7, 8, 11, 13, 14\}$ Let us determine their orders.

In fact, since $|(\mathbb{Z}/15\mathbb{Z})^\times| = 8$ and the order of an element divides the cardinality of the group, we know that all elements have order 2^k for some $k \in \{0, -, 3\}$.

In particular, all elements of $(\mathbb{Z}/15\mathbb{Z})^\times$ except $\overline{1}$ have even order.

We can compute it:

element a	order r
2	4
4	2
7	4
8	4
11	2
13	4
14	2

2. Let's see which of these element also satisfies $a^{\frac{r}{2}} \not\equiv -1 \pmod{15}$

element a	$a^{r/2} \pmod{15}$
2	4
4	4
7	4
8	4
11	11
13	4
14	-1

So $14 = -1$ is the only element in $(\mathbb{Z}/15\mathbb{Z})^\times$ which does not satisfy $a^{r/2} \not\equiv -1 \pmod{15}$

The proportion of elements of $(\mathbb{Z}/15\mathbb{Z})^\times$ which satisfy A1 and A2 is $7/8$.

In the next exercise, we prove a general result on the proportion of elements satisfying A1 and A2.

Ex 2:

1. Let a be a generator of the cyclic group $(\mathbb{Z}/p\mathbb{Z})^\times$.

Then $(\mathbb{Z}/p\mathbb{Z})^\times = \{a^k,\ k \in \{1, \dots, p-1\}\}$

Now $\operatorname{ord}(a^k) = \dfrac{\operatorname{ord}(a)}{\gcd(\operatorname{ord}(a), k)} = \dfrac{p-1}{\gcd(p-1, k)}$ ← even

$p-1$: even; k: we can choose.

For any k that is odd, $\gcd(p-1, k)$ will be odd, so $\operatorname{ord}(a^k)$ will be even. So for all $j \in \{0, \dots, \frac{p-1}{2} - 1\}$,

a^{2j+1} is an element of $(\mathbb{Z}/p\mathbb{Z})^\times$ of even order.

This gives a list of $\frac{p-1}{2}$ elements of even order in $(\mathbb{Z}/p\mathbb{Z})^\times$.
(They are distinct because since a has order $p-1$, $a^1, \dots, a^{p-1}$ are distinct).

2. If p is any prime number, $\mathbb{Z}/p\mathbb{Z}$ is a field, so the polynomial $X^2 - 1$ has at most two (= degree of the polynomial) roots in $(\mathbb{Z}/p\mathbb{Z})$. Moreover, if p is odd, $-1 \neq +1$ in $\mathbb{Z}/p\mathbb{Z}$, so $X^2 - 1$ has exactly two roots.

3. Recall that $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ is cyclic (because p is odd) of order $(p-1)p^{\alpha-1} = \varphi(p^\alpha)$. We can use the same argument as above: Let a be a generator of $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$. Then for all k,

$$\operatorname{ord}(a^k) = \frac{(p-1)p^{\alpha-1}}{\gcd(k, (p-1)p^{\alpha-1})}$$ so that for all odd k,

$\mathrm{ord}(a^k)$ will be even (because $p-1$ is even).

Therefore $\left\{ a^{2j+1},\ 0 \le j \le \frac{(p-1)p^{\alpha-1}}{2} - 1 \right\}$ are distinct elements of $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ of even order. So at least half of the elements of $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ have even order.

Concerning the number of solutions to the equation $x^2 = 1$:

⚠ now $\mathbb{Z}/p^\alpha\mathbb{Z}$ is not a field if $\alpha \ge 2$, so the argument with the number of roots of the polynomial $X^2 - 1$ no longer works

Let a be a generator of $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$. Let (b, c) be its image under the isomorphism of the Chinese remainder theorem:

$$\underbrace{(\mathbb{Z}/p^\alpha\mathbb{Z})^\times}_{\text{cyclic of order } (p-1)p^{\alpha-1}} \simeq \underbrace{\mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}/p^{\alpha-1}\mathbb{Z}}_{\text{as additive groups}}$$

Then $\forall k \in \{0, \dots, (p-1)p^{\alpha-1} - 1\}$,

$$(a^k)^2 \equiv 1 \pmod{p^\alpha} \iff \begin{cases} 2kb \equiv 0 \pmod{p-1} \\ 2kc \equiv 0 \pmod{p^{\alpha-1}} \end{cases}$$

$$\iff \begin{cases} \mathrm{ord}(b) \mid 2k \\ \mathrm{ord}(c) \mid 2k \end{cases}$$

Since a is a generator, b and c are generators

$$\iff \begin{cases} p-1 \mid 2k \\ p^{\alpha-1} \mid 2k \end{cases} \iff \begin{cases} \frac{p-1}{2} \mid k \\ p^{\alpha-1} \mid k \end{cases}$$ because p is odd

Now if $\alpha = 1$, $p^{\alpha-1}$ and $\frac{p-1}{2}$ are coprime.

if $\alpha > 1$, $p^{\alpha-1}$ and $\frac{p-1}{2}$ are coprime because $p \nmid \frac{p-1}{2}$

So $(a^k)^2 \equiv 1 \pmod{p^\alpha} \iff \frac{p-1}{2} \times p^{\alpha-1} \mid k$.

$\iff k \in \{0,\ \frac{p-1}{2} \times p^{\alpha-1}\}$

So there are only two roots of 1 in $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$,

$$a^0 = 1 \quad \text{and} \quad a^{\frac{p-1}{2} p^{\alpha-1}} = -1.$$

4. The ring isomorphism of the CRT induces a group isomorphism

$$\left(\mathbb{Z}/n\mathbb{Z}\right)^\times \simeq \left(\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z}\right)^\times \times \cdots \times \left(\mathbb{Z}/p_\ell^{\alpha_\ell}\right)^\times$$

$$a \longmapsto (a_1, \ldots, a_\ell)$$

Moreover, for all $k \in \mathbb{Z}$,

$$a^k \equiv 1 \pmod{n} \iff \forall i \in [\![1,\ell]\!],\ a_i^k \equiv 1 \pmod{p_i^{\alpha_i}}$$

$$\iff \forall i \in [\![1,\ell]\!],\ \mathrm{ord}(a_i) \mid k$$

$$\iff \mathrm{lcm}(\mathrm{ord}(a_1), \ldots, \mathrm{ord}(a_\ell)) \mid k$$

Thus, $\boxed{\mathrm{ord}(a) = \mathrm{lcm}(\mathrm{ord}(a_1), \ldots, \mathrm{ord}(a_\ell))}$

Therefore $\mathrm{ord}(a)$ is odd <u>iff</u> $\forall i \in [\![1,\ell]\!]$, $\mathrm{ord}(a_i)$ is odd.

(ie $\mathrm{ord}(a)$ is even <u>iff</u> $\exists i \in [\![1,\ell]\!]$, $\mathrm{ord}(a_i)$ is even)

Now thanks to the case of $n=p^\alpha$, we know that the proportion of $a_i \in (\mathbb{Z}/p^{\alpha_i}\mathbb{Z})^\times$ such that $\mathrm{ord}(a_i)$ is odd is $\leqslant \frac{1}{2}$

Therefore, $\#\{(a_1,\dots,a_\ell) \in \prod (\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z})^\times$ such that $\forall i$, $\mathrm{ord}(a_i)$ is odd$\}$

$$\leqslant \frac{p_1^{\alpha_1-1}(p_1-1)}{2} \times \cdots \times \frac{p_\ell^{\alpha_\ell-1}(p_\ell-1)}{2}$$

$$= \frac{\varphi(n)}{2^\ell}$$

So $$\frac{\#\{a \in (\mathbb{Z}/n\mathbb{Z})^\times, \ \mathrm{ord}(a) \text{ is odd}\}}{\varphi(n)} \leqslant \frac{1}{2^\ell}$$

We conclude that the proportion of elements of $(\mathbb{Z}/n\mathbb{Z})^\times$ that have even order is $\geqslant 1-\frac{1}{2^\ell}$

5. Consider again the isomorphism

$$(\mathbb{Z}/n\mathbb{Z})^\times \simeq (\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/p_\ell^{\alpha_\ell}\mathbb{Z})^\times$$

$$a \longmapsto (a_1, \dots, a_\ell)$$

Then $a^2 \equiv 1 \pmod n \iff \forall i \in [\![1,\ell]\!],\ a_i^2 \equiv 1 \pmod{p_i^{\alpha_i}}$

$$\overset{q^\circ 3}{\iff} \forall i \in [\![1,\ell]\!],\ a_i \in \{\pm 1\} \pmod{p_i^{\alpha_i}}$$

$\Rightarrow$ there are 2^ℓ square roots of 1 in $(\mathbb{Z}/n\mathbb{Z})^\times$.

Ex 3 : 1. ⇐ Assume that all v_i are equal to the same value.

- If they are all equal to zero, then all order r_i are odd, so $\text{ord}(x) = \text{lcm}(r_1, \dots, r_\ell)$ is odd, so x does not satisfy A1.

- If they are all equal to some $\omega \geq 1$, then

$$r_1 = 2^\omega s_1, \dots, r_\ell = 2^\omega s_\ell \quad \text{with } s_1, \dots, s_\ell \text{ odd.}$$

So $r = \text{lcm}(r_1, \dots, r_\ell) = 2^\omega \text{lcm}(s_1, \dots, s_\ell)$ has 2-adic valuation ω.

Then $x^{r/2}$ is mapped by the Chinese Remainder Theorem to

$$(x_1^{r/2}, \dots, x_\ell^{r/2}) = (x_1^{2^{\omega-1} s_1}, \dots, x_\ell^{2^{\omega-1} s_\ell})$$

and for all i, $x_i^{2^{\omega-1} s_i}$ is a square root of 1, but is not equal to 1, so it is -1 thanks to ex 2.

Therefore, $x^{r/2} \equiv -1 \pmod n$ so x does not satisfy A2.

⇒ Take the contrapositive: we assume that the v_i are not all equal and we want to show that x satisfies A1 and A2.

Without loss of generality let's assume that $v_2 > v_1$.

Then $r = \text{lcm}(2^{v_1} s_1, 2^{v_2} s_2, \dots, 2^{v_\ell} s_\ell)$ is a multiple of $2^{v_2} s_2$

so $v \geq v_2$. and $r = 2^v s$ where $s = \text{lcm}(s_1, \dots, s_\ell)$

(in ticular r is even, so A1 is satisfied.

So $x^{r/2}$ corresponds via the Chinese Remainder Theorem to

$$\left(x_1^{r/2}, \dots, x_\ell^{r/2}\right) = \left(x_1^{2^{v-1}s}, x_2^{2^{v-1}s}, \dots, x_\ell^{2^{v-1}s}\right)$$

$$= (1, *, \dots, *) \neq (-1, -1, \dots, -1)$$

↑

because $v \geq v_2 > v_1$

So $2^{v-1}s$ is a multiple

of $2^{v_1}s_1 = r_1$

So $x^{r/2} \not\equiv -1 \pmod n$ hence A2 is satisfied.

2. As in Ex2 we use the fact that $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ is a cyclic group and pick a generator a.

Then $$\mathrm{ord}(a^k) = \frac{\mathrm{ord}(a)}{\gcd(k, \mathrm{ord}(a))} = \frac{\varphi(p^\alpha)}{\gcd(k, \varphi(p^\alpha))}$$

$$= \frac{(p-1)p^{\alpha-1}}{\gcd((p-1)p^{\alpha-1}, k)}$$

Denote by γ the 2-adic valuat° of $p-1$

Then $$v_2(\mathrm{ord}(a^k)) = \gamma - v_2(\gcd((p-1)\underbrace{p^{\alpha-1}}_{\text{odd}}, k))$$

$$= \gamma - v_2(\gcd(p-1, k))$$

So $v_2(\mathrm{ord}(a^k)) = \beta \iff v_2(\gcd(p-1, k)) = \gamma - \beta$

- Therefore, if $\gamma-\beta<0$, there is no such k, so the proportion of elements whose 2-adic valuation equals β is equal to 0.
(it was also clear from the fact that the order of an element must divide the cardinality of the group, which here is equal to $(p-1)p^{\alpha-1}$, with 2-adic valuation $=\gamma$).

- if $\gamma-\beta\geq 0$, then $v_2(\gcd(p-1,k)) = \gamma-\beta$

iff k is of the form $2^{\gamma-\beta}t$ for some odd integer t.

How many integers $k\in\{0,\dots,\varphi(p^\alpha)-1\}$ are of the form $2^{\gamma-\beta}t$ with t odd?

It is always less than or equal to the number of odd integers t in $\{0,\dots,\varphi(p^\alpha)-1\}$ which is $\frac{\varphi(p^\alpha)}{2}$.

So in any case, we obtain the result.

3. Via the Chinese Remainder Theorem, the $x\in(\mathbb{Z}/n\mathbb{Z})^\times$ that DO NOT satisfy A1 and A2 correspond to the elements $(x_1,\dots,x_\ell)$ in $\prod_{i=1}^{\ell}(\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z})^\times$ such that for all $i\in\{2,\dots,\ell\}$,

$v_2(\mathrm{ord}(x_i)) = v_2(\mathrm{ord}(x_1))$ (thanks to question 1.)

So $\#\{x\in(\mathbb{Z}/n\mathbb{Z})^\times$ such that x doesn't satisfy A1 and A2$\}$ is in 1 to 1 correspondence with

$$\bigsqcup_{x_1\in(\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z})^\times}\{(x_1,x_2,\dots,x_\ell)\in\prod_{i=1}^{\ell}(\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z})^\times,\ \text{for all } i\geq 2,\ v_2(\mathrm{ord}(x_i))=v_2(\mathrm{ord}(x_1))$$

So its cardinality is

$$\sum_{a_1 \in (\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z})^\times} \#\left\{(x_2,\dots,x_\ell) \in \prod_{i=2}^{\ell} (\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z})^\times,\ v_2(\mathrm{ord}(x_i)) = v_2(\mathrm{ord}(x_1))\right\}$$

$\varphi(p_1^{\alpha_1})$ terms

$$\leq \prod_{i=2}^{\ell} \frac{\varphi(p_i^{\alpha_i})}{2}$$ thanks to question 2

So $$\frac{\#\{x \in (\mathbb{Z}/n\mathbb{Z})^\times \text{ such that } x \text{ does not satisfy A1 and A2}\}}{\varphi(n)} \leq \frac{1}{2^{\ell-1}}$$

hence the conclusion.

Ex5: $75 = 14 \times 5 + 5 \iff \frac{75}{14} = 5 + \frac{5}{14} = 5 + \frac{1}{\frac{14}{5}} = 5 + \frac{1}{2 + \frac{4}{5}} = 5 + \frac{1}{2 + \frac{1}{1 + \frac{1}{4}}}$

$14 = 5 \times 2 + 4 \iff \frac{14}{5} = 2 + \frac{4}{5}$

$5 = 4 \times 1 + 1 \iff \frac{5}{4} = 1 + \frac{1}{4}$

So $\frac{75}{14}$ is represented by the list $[5, 2, 1, 4]$

This gives the successive approx:

$[5] : 5$

$[5,2] : 5 + \frac{1}{2} = \frac{11}{2} = 5,5$

$[5,2,1] = 5 + \frac{1}{2 + \frac{1}{1}} = 5 + \frac{1}{3} = \frac{16}{3} = 5,33\ldots$

$[5,2,1,4] = \frac{75}{14} = 5,357142 8\ldots$