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 $< \frac{1}{2}$

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$\}$

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

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

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

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

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 $(\mathbb{Z}/n\mathbb{Z})^\times$.

Ex3: 1. Let $y \in (\mathbb{Z}/n\mathbb{Z})^\times$. Denote by $A_y := \{x \in (\mathbb{Z}/n\mathbb{Z})^\times,\ x^5 = y^5\}$.

$\forall x \in (\mathbb{Z}/n\mathbb{Z})^\times,\quad x^5 \equiv y^5 \pmod n \iff \left(\frac{x}{y}\right)^5 \equiv 1 \pmod n$

So $\quad x \in A_y \iff \frac{x}{y} \in A_1$

So for all $y \in (\mathbb{Z}/n\mathbb{Z})^\times,\quad |A_y| = |A_1|$.

2. Consider the isomorphism $(\mathbb{Z}/n\mathbb{Z})^\times \xrightarrow{\sim} \left(\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z}\right)^\times \times \cdots \times \left(\mathbb{Z}/p_\ell^{\alpha_\ell}\mathbb{Z}\right)^\times$

$z \longmapsto (z_1, \ldots, z_\ell)$

Then $z \in R \iff \forall i \in [\![1,\ell]\!],\ z_i^2 \equiv 1 \pmod{p_i^{\alpha_i}}$

$\iff \forall i \in [\![1,\ell]\!],\ z_i \in \{\pm 1\} \pmod{p_i^{\alpha_i}}$

Now if x_0 satisfies $x_0^5 \equiv -1 \pmod n$, then its image $x_1^5, \ldots, x_\ell^5$ in $\left(\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z}\right)^\times \times \cdots \times \left(\mathbb{Z}/p_\ell^{\alpha_\ell}\mathbb{Z}\right)^\times$ is $(-1, \ldots, -1)$

Therefore, it suffices to define $(y_1, \ldots, y_\ell)$ by

$$\begin{cases} y_i = 1 & \text{if } z_i = 1 \\ y_i = x_i & \text{if } z_i = -1 \end{cases}$$

Then $(y_1^5, \ldots, y_\ell^5) = (z_1, \ldots, z_\ell)$ so the element y of $(\mathbb{Z}/n\mathbb{Z})^\times$ corresponding to $(y_1, \ldots, y_\ell)$ via the isomorphism of the CRT satisfies $y^5 \equiv z \pmod n$.

3. • If $x^s \equiv -1 \pmod n$ has no solut^{s} in $(\mathbb{Z}/n\mathbb{Z})^\times$, then $S_s = S'_s$

so $$\frac{|S'_s|}{|S_s|} = 1 \geq 1 - \frac{1}{2^\ell - 1}$$

• Otherwise, let x_0 be such that $x_0^s \equiv -1 \pmod n$. Let $z \in R$.
Then thanks to the previous question, there exists $y \in (\mathbb{Z}/n\mathbb{Z})^\times$ such that $z = y^s$.

Therefore, the equat^{n} $x^s = z$ is equivalent to $x^s = y^s$, so by q^{o} 1, the number of solut^{s} does not depend on y, hence on z.
Let us denote by d this number of solut^{s}.

Then $$S_s = \bigsqcup_{z \in R \setminus \{1\}} \{x \in (\mathbb{Z}/n\mathbb{Z})^\times,\ x^s = z\}$$

$$S'_s = \bigsqcup_{z \in R \setminus \{-1,1\}} \{\text{---------}\}$$

So $$\begin{cases} |S_s| = d \times \mathrm{Card}(R \setminus \{1\}) = d(2^\ell - 1) \\ |S'_s| = d \times \mathrm{Card}(R \setminus \{-1,1\}) = d(2^\ell - 2) \end{cases}$$

hence $$\frac{|S'_s|}{|S_s|} = \frac{2^\ell - 2}{2^\ell - 1} = 1 - \frac{1}{2^\ell - 1}$$

4. We saw in Ex 2 that the number E_n of elements of <u>even</u> order in $(\mathbb{Z}/n\mathbb{Z})^\times$ satisfies $$\frac{E_n}{\varphi(n)} > 1 - \frac{1}{2^\ell} = \frac{2^\ell - 1}{2^\ell}.$$

Now, to each element a of even order r, we denote $s := \frac{r}{2}$.

Then $(a^s)^2 = a^r = 1$ so $a^s \in R$

but $a^s \neq 1$ (otherwise it would contradict the minimality of r)

Thus, $a \in S_s$. This shows that the set of elements a in $(\mathbb{Z}/n\mathbb{Z})^\times$ of even order is the union of the S_s for $s \in \{1, \dots, \frac{\varphi(n)}{2}\}$. Moreover, this union is disjoint by uniqueness of the order.

Now, denote by $\mathcal{F}_n := \{x \in (\mathbb{Z}/n\mathbb{Z})^\times,\ \mathrm{ord}(x) \text{ is even and } x^{\frac{\mathrm{ord}(x)}{2}} \not\equiv -1 \pmod n\}$

then $\mathcal{F}_n = \bigsqcup_{s=1}^{\varphi(n)/2} S'_s$

So its cardinality $F_n = |\mathcal{F}_n|$ satisfies:

$$F_n = \sum_{s=1}^{\varphi(n)/2} |S'_s| = \sum_{s=1}^{\varphi(n)/2} \underbrace{\frac{|S'_s|}{|S_s|}}_{\geq \frac{2^l-2}{2^l-1}} \times |S_s| \geq \frac{2^l-2}{2^l-1} \underbrace{\sum_{s=1}^{\varphi(n)/2} |S_s|}_{E_n}$$

So $$\frac{F_n}{\varphi(n)} \geq \frac{2^l-2}{2^l-1} \underbrace{\frac{E_n}{\varphi(n)}}_{> \frac{2^l-1}{2^l}} > \frac{2^l-2}{2^l} = 1 - \frac{1}{2^{l-1}}$$

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:

$[5] : 5$

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

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

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