Number Theory

Martina Tscheckl

October 10, 2015

Contents

Organizatorial stuff

Dates (in TUGrazOnline):

Mon	14:15–15:45	C208	Exercises (starting 19.10. first exercise class)
Tue	14:15–15:45	C307	Lecture (starting 20.10. first (real) lecture)
Wed	08:15–09:45	C208	Lecture

From now until 15.12. lectures by Martin Widmer. Then C. Frei.
End: oral exams
Exercises: Find details on website of the instructor Dijana Kreso. math.tugraz.at/~kreso

0 Basics

$$\mathbb{N} = \{1, 2, \dots\} \tag{1}$$
$$\mathbb{N}_0 = \mathbb{N} \cup \{0\} \tag{2}$$

0.1 Divisibility

Definition 1. *Let $a, b \in \mathbb{Z}$. a divides b (written $a \mid b$) if $\exists q \in \mathbb{Z} : b = qa$.*
Some properties: Let $a, b, c \in \mathbb{Z}$. Then the following statements hold:

$$a \mid b \Rightarrow ac \mid bc \tag{3}$$
$$a \mid b \wedge b \mid c \Rightarrow a \mid c \tag{4}$$
$$a \mid b \wedge b \mid a \Leftrightarrow a = b \tag{5}$$
$$a \mid b \wedge a \mid c \Rightarrow a \mid (b + c) \tag{6}$$

Definition 2 (Remainder)**.** *Let $a \in \mathbb{Z}$, $b \in \mathbb{N}$. Then there are unique $q, r \in \mathbb{Z}$ such that:*

$$a = qb + r \text{ and } 0 \leq r < b$$

Remark 1.

1. *$b \mid a \Leftrightarrow r = 0$*
2. *$q = \lfloor \frac{a}{b} \rfloor$ (largest integer $\leq \frac{q}{b}$)*
3. *we will somtimes write: $a \mod b := c$*

Definition 3. *Let $a_1, a_2, \ldots, a_n, d \in \mathbb{Z}$. d is a greatest common divisor (gcd) of $a_1, \ldots, a_n$ if $d \mid a_i$ $\forall 1 \leq a_i \leq n$ and if $e \in \mathbb{Z}$ such that $e \mid a_i$ $\forall 1 \leq i \leq n$, then $e \mid d$*

Remark 2.

1. *a $\gcd$ of $a_1, \ldots, a_n$ is unique up to sign*
2. *we write $d = \gcd(a_1, \ldots, a_n)$ if d is a $\gcd$ of $a_1, \ldots, a_n$*
3. *for $a_1, \ldots, a_n \in \mathbb{Z}$, a $\gcd$ exists and can be written as a linear combination of $a_1, \ldots, a_n$ i.e., $\exists x_1, \ldots, x_n \in \mathbb{Z}$ such that $\gcd(a_1, \ldots, a_n) = x_1 a_1 + \cdots + x_n a_n$*
4. *$\gcd(a_1, \ldots, a_n) = \gcd(\gcd(a_1, \ldots, a_{n-1}), a_n)$*
5. *if $a \mid bc$ and $\gcd(a, b) = 1$ then $a \mid c$.*
6. *let $a' := \frac{a}{\gcd(a,b)}$, $b' = \frac{b}{\gcd(a,b)}$. Then $\gcd(a', b') = 1$*

Algorithm 1 Compute the gcd of two integers: Euclidean algorithm

---

Given: $a, b \in \mathbb{Z}$. $|a| \geq |b|$
Find: $a := \gcd(a, b)$
  replace a by $|a|$, b by $|b|$
  while $b \neq 0$ **do**
    write $a = qb + r$, $0 \leq r < b$
    $a := b$
    $b := r$
  end while
  return a

The algorithm is correct, since $\gcd(a, b) = \gcd(b, a \mod b)$.
The algorithm terminates because b decreases in each step.
The algorithm is fast: $(\mathcal{O}(\log b))$

The Euclidean algorithm also allows us to find x, y such that $\gcd(a, b) = ax + by$ by doing all computations backwards.

Example 1. $\gcd(56, 22) = ?$

$$\begin{aligned}
a &= 56, b = 22 \\
56 &= 2 \cdot 22 + 12 \\
a &= 22, b = 12 \neq 0 \\
22 &= 1 \cdot 12 + 10 \\
a &= 12, b = 10 \neq 0 \\
12 &= 1 \cdot 10 + 2 \\
a &= 10, b = 2 \neq 0 \\
10 &= 5 \cdot 2 + 0 \\
a &= 2, b = 0 && \Rightarrow \gcd(56, 22) = 2
\end{aligned}$$

Doing the computations backwards:

$$\begin{aligned}
&2 = 12 - 10 = 12 - (22 - 12) = -22 + 2 \cdot 12 = -22 + 2(56 - 2 \cdot 22) = 2 \cdot 56 - 5 \cdot 22 \\
&x = 2, y = -5
\end{aligned}$$

Application (linear diophantine equations)**.** *Let* $a, b, c \in \mathbb{Z}$*,* $a, b, c \neq 0$*. Find all* $(x, y) \in \mathbb{Z}^2$ *which satisfy*

$$ax + by = c \tag{7}$$

Existence of solution let $d = \gcd(a, b)$.

$$\begin{aligned}
(d \mid a \Rightarrow d \mid xa) &\wedge (d \mid b \Rightarrow d \mid yb) \\
&\Rightarrow d \mid xa + yb = c \\
&\Rightarrow \textit{eq. } (7)
\end{aligned}$$

can have solutions only if $d \mid c$.

Solution in case $d = 1$ Let $x_0, y_0 \in \mathbb{Z}$ such that $ax_0 + by_0 = 1$ using the Euclidean algorithm. Then from $acx_0 + bcy_0 = c$ the solution (cx_0, cy_0) of (eq. (7)) follows: for all $n \in \mathbb{Z} : (x, y) := (cx_0 + nb, cy_0 + na)$ is a solution.

Indeed,

$$ax + by = acx_0 + anb + bcy_0 - bna = c \qquad \checkmark$$

These (x, y) are all solutions: let (x, y) be a solution. Then

$$\begin{aligned}
ax + by &= c \\
acx_0 + bcy_0 &= c \\
\Rightarrow a(x - cx_0) &= b(cy_0 - y) \\
\gcd(a, b) = 1 \;\Rightarrow\; b \mid x - cx_0 \;&\Rightarrow\; x = cx_0 + nb, n \in \mathbb{Z} \\
\Rightarrow\; a \mid cy_0 - y \;&\Rightarrow\; y = cy_0 + ma, m \in \mathbb{Z} \\
c = ax + by &= acx_0 + anb + bcy_0 + bma \\
= c + (n + m)ab &\Rightarrow (n + m)ab = 0 \Rightarrow m = -n
\end{aligned}$$

Solutions in the general case Assume $d = \gcd(a, b)$ and $d \mid c$, let

$$a' = \frac{a}{d} \qquad b' = \frac{b}{d} \qquad c' := \frac{c}{d}$$

Then $\gcd(a', b') = 1$ and the solution to (eq. (7)) is exactly the solution of $a'x + b'y = c'$.

0.2 Primes

Definition 4. *$p \in \mathbb{N}$, $p > 1$ is a* prime number *if the only positive divisors of p are 1 and p i.e. $a \in \mathbb{N}$, $a \mid p \Rightarrow a \in \{1, p\}$. $\mathbb{P} := \{primes\} \subset \mathbb{N}, \mathbb{P} = \{2, 3, 5, 7, 11, 13, \dots\}$. p prime and $p \mid ab \Rightarrow p \mid a$ or $p \mid b$*

Theorem 1 (Fundamental theorem of arithmetic)**.** *Every $n \in \mathbb{N}$ can be written uniquely (up to reordering) as a product of primes. i.e. there are distinct primes $p_1, \dots, p_l$, and $\alpha_1, \dots, \alpha_l \in \mathbb{N}$ such that $n = p_1^{\alpha_1} \dots p_l^{\alpha_l}$*

Sketch.

Existence let $p_0 > 1$ be the smallest divisor > 1 of n. Then p_0 is prime. $n = p_0 n_0$, induction ✓

Uniqueness let $p_1 \dots p_m = q_1 \dots q_l = n$, p_i, q_j primes. $p_1 \mid q_1 \dots q_l \Rightarrow \exists i : p_1 \mid q_i$, both prime $\Rightarrow p_1 = q_i$, wlog: $i = 1$. $p_1 \dots p_m = q_1 \dots q_l$, induction ✓

□

Theorem 2 (Euclid)**.** *There are ∞-many primes.*

Proof. Given primes $p_1, \dots, p_n \in \mathbb{P}$. We construct one more prime

$$N := p_1 \cdot \dots \cdot p_n + 1.$$

Assume P is a prime factor of N. If $P \in \{p_1, \dots, p_n\}$ then $P \mid N$ and $P \mid p_1 \dots p_n \Rightarrow P \mid 1$ ↯ □

Remark 3 (prime factors and gcds)**.** *Let $a_1, \dots, a_n \in \mathbb{Z}$, write*

$$a_i = \prod_{p \in \mathbb{P}} p^{\alpha_{p,i}}, \ \alpha_{p,i} \in \mathbb{N}_0,$$

almost all $a_i = 0$, then

$$\gcd(a_1, \dots, a_n) = \prod_{p \in \mathbb{P}} p^{\min_{1 \le i \le n} \{\alpha_{p,i}\}}$$

0.3 Congruences

All rings are commutative with 1.

Definition 5. *Let $a, b \in \mathbb{Z}$, $n \in \mathbb{N}$. Then a* is congruent to *$b \pmod n$, $a \equiv b \pmod n$, if $n \mid a - b$. We write $\bar{a} = [a]_n := \{b \in \mathbb{Z} : b \equiv a (\mod n)\}$*

Remark 4.

1. *Congruence* mod$n$ *is an* equivalence relation
2. *$\bar{0}, \bar{1}, \dots, \overline{n-1}$ is a partition of $\mathbb{Z}$.*
3. *if $a \equiv b \pmod n$, $c \equiv d \pmod n$, then $-a \equiv -b \pmod n$, $a \stackrel{+}{\underset{-}{\cdot}} d \pmod n$.*

Definition 6. *$\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n := \{[a]_n : a \in \mathbb{Z}\} = \{\bar{0}, \bar{1}, \dots, \overline{n-1}\}$ residue class ring modulo n*

Remark 5. *$\mathbb{Z}_n$ is a ring with operation $\bar{a} \stackrel{+}{\underset{-}{\cdot}} \bar{b} := \overline{a \stackrel{+}{\underset{-}{\cdot}} b}$ (well defined due in item 3 of Remark 4) $\mathbb{Z}_n^\times = \{\bar{a} \in \mathbb{Z}_n : \exists \bar{b} \in \mathbb{Z}_n : \bar{a}\bar{b} = \bar{1}$ ... group of units* $\mod n$

Lemma 1. *Let $a \in \mathbb{Z}$. Then $\bar{a} \in \mathbb{Z}_n^\times \Leftrightarrow \gcd(a,n) = 1$.*

Proof.

"$\Rightarrow$" $\bar{a}\bar{b} = \bar{1} \Leftrightarrow ab \equiv 1 \pmod{n} \Leftrightarrow n \mid ab - 1$
$\Rightarrow$ no prime factor of n divides a
$\Rightarrow \gcd(a,n) = 1$.

"$\Leftarrow$" $1 = \gcd(a,n) = ax + ny \Rightarrow \bar{1} = \bar{a}\bar{x}$

□

Remark 6. *The inverse of $\bar{a}$ can be computed by the Euclidean algorithm.*

Example 2 (Simultaneous congruences)**.** *Find $x \in \mathbb{Z}$ such that*

$$x \equiv 2 \pmod{3} \tag{8}$$
$$x \equiv 1 \pmod{5} \tag{9}$$
$$x \equiv 0 \pmod{7} \tag{10}$$

Theorem 3 (Chinese remainder theorem (CRT))**.** *Let*

$$n_1, \dots, n_l \in \mathbb{N} \text{ subject to } \gcd(n_i, n_j) = 1 \ \forall i \neq j$$

$$x_1, \dots, x_l \in \mathbb{Z}.$$

Then

$$\exists x \in \mathbb{Z} \text{ such that } x \equiv x_i \pmod{n_i} \ \forall 1 \leq i \leq l$$

where x is unique modulo $n_1 \cdot \dots \cdot n_l$.

Proof. How to compute x? For $i \in \{1, \dots, l\}$, let

$$N_i := \prod_{j \neq i} n_j = n_1 \dots n_{i-1} n_{n+1} \dots n_l$$

and let

$$N := \prod_i n_i = n_1 N_1 = n_2 N_2 = \dots = n_l N_l$$

because $\gcd(n_i, N_i) = 1 \Rightarrow N_i$ in invertible modn_i. Let

$$m_i N_i \equiv 1 \pmod{n_i}$$

and let

$$x := N_1 m_1 x_1 + \dots + N_l m_l x_l.$$

We have $N_i m_i x_i \equiv 0 \pmod{n_j, j \neq i}$ □

Example 3.

$$n_1 = 3, \qquad n_2 = 5, \qquad n_3 = 7$$

$$x_1 = 2, \qquad x_2 = 1, \qquad x_3 = 0$$

$$N_1 = 35, \qquad N_2 = 21, \qquad N_3 = ?$$

$$\overline{m}_1 = \overline{35}^{-1} \pmod{3} = \bar{2}^{-1} \pmod{3} = \bar{2} \pmod{3} \Rightarrow m_1 = 2$$

$$\overline{m}_2 = \overline{21}^{-1} \pmod{5} = \bar{1}^{-1} \pmod{5} = \bar{1} \pmod{5} \Rightarrow m_2 = 1$$

$$\begin{aligned} x &= 35 \cdot 2 \cdot 2 + 21 \cdot 1 \cdot 1 + 0 \\ &= 140 + 21 \\ &= 161 \\ &\equiv 56 \pmod{105} \end{aligned}$$

Example 4 (more abstract CRT). *Let* $n_1, \ldots, n_l \in \mathbb{N}$*, with* $\gcd(n_i, n_j) = 1$ $\forall i \neq j$*. There is a ring isomorphism* $f : \mathbb{Z}_{n_1 \ldots n_l} \overset{\cong}{\mapsto} \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_l}$ *that satisfies* $f([a]_{n_1 \ldots n_l}) = ([a]_{n_1}, \ldots, [a]_{n_l})$ $\forall a \in \mathbb{Z}$*. In particular:* $\mathbb{Z}^\times_{n_1 \ldots n_l} \cong \mathbb{Z}^\times_{n_1} \times \cdots \times \mathbb{Z}^\times_{n_l}$ *(restrict* f *to* $\mathbb{Z}^\times_{n_1 \ldots n_l}$*)*

0.4 Arithmetic functions

Definition 7. $f : \mathbb{N} \to \mathbb{C}$ *is an* arithmetic function*.* f *is* multiplicative *if* $\forall m, n$ *it holds that* $\gcd(m,n) = 1$*. We have* $f(mn) = f(m)f(n)$*.* f *is* completely multiplicative *if* $\forall m, n : f(mn) = f(m)f(n)$*. Let* $f : \mathbb{N} \to \mathbb{C}$*. Its* summatory function *is* $S_f(n) := \sum_{d \mid n} f(d)$*.*

Proof. If $\gcd(m,n) = 1$ and $d \mid mn$, then $\exists$ unique d_1, d_2 such that $d = d_1 \cdot d_2$ with $d_1 \mid m$, $d_2 \mid n$.

$$S_f(mn) = \sum_{d \mid mn} f(d) = \sum_{d_1 \mid m} \sum_{d_2 \mid n} f(d_1 d_2) = \sum_{d_1 \mid m} f(d_1) \sum_{d_2 \mid n} f(d_2) = S_f(m) S_f(n)$$

□

Example 5.

$$\tau(n) := S_1(n) = \sum_{d \mid n} 1 \qquad \ldots \textit{number of divisors of } n$$

$$\sigma(n) := S_{id}(n) = \sum_{d \mid n} d \qquad \ldots \textit{divisor sum of } n$$

Definition 8. *The function* $\phi(n) := |\mathbb{Z}^\times_n|$ *is called* Euler's ϕ-function*.*

Remark 7.

1. $\phi(n) = |\{0 \le a < n : \gcd(a,n) = 1\}|$
2. ϕ *is multiplicative (CRT:* $\gcd(m,n) = 1$*.* $\mathbb{Z}^\times_{nm} \cong \mathbb{Z}^\times_n \times \mathbb{Z}^\times_m$*)*
3. $\phi(p) = p - 1$ *(*$\mathbb{Z}_p$ *is a field)*

Lemma 2. $\phi(p^n) = p^n - p^{n-1}$

Proof.

$$\begin{aligned} \phi(p^n) &= |\{0 \le a < p^n\}| - |\{0 \le a < p^n : \gcd(a, p^n) \neq 1\}| \\ &= p^n - |\{0 \le a < p^n : p | a\}| \\ &= p^n - p^{n-1} \end{aligned}$$

□

Proposition 1. *If* $n = p_1^{\alpha_1} \ldots p_l^{\alpha_l}$ *with* $p_i \neq p_j$ *primes,* $\alpha_i \in \mathbb{N}$*. Then*

$$\phi(n) = \prod_{i=1}^{l} p_i^{\alpha_i} (1 - \frac{1}{p_i}) = n \prod_{p \mid n} (1 - \frac{1}{p})$$

Theorem 4 (Euler-Fermat)**.** *Then* $a^{\phi(n)} \equiv 1 \mod n$*. In particular:* $a^{p-1} \equiv 1 \mod p\ \forall p \nmid a$ *(little Fermat).*

Proof 1. Lagrange's Theorem, $G = \mathbb{Z}_n^\times, \bar{a} \in G \Rightarrow \bar{a}^{|G|} = \bar{1}, |G| = \phi(n)$. ☐

Proof 2. $\prod_{x \in \mathbb{Z}_n^\times} x = \prod_{x \in \mathbb{Z}_n^\times} (\bar{a}x) = \bar{a}^{\phi(n)} \prod_{x \in \mathbb{Z}_n^\times} x \Rightarrow a^{\phi(n)} \equiv 1 \mod n$ ☐

Definition 9. *The Möbius function* $\mu : \mathbb{N} \to \{-1, 0, +1\}$ *is defined as*

$$\mu(n) = \begin{cases} (-1)^l & n = p_1 \dots p_l, p_i \neq p_j, i \neq j, p_i \textit{ primes} \\ 0 & \textit{otherwise i.e. if } \exists p : p^2 \mid n \end{cases}$$

Remark 8.

1. $\mu(1) = 1,\ \mu(2) = -1,\ \mu(3) = -1,\ \mu(4) = 0,\ \mu(5) = -1,\ \mu(6) = 1,\ \dots$
2. μ *is* multiplicative

Lemma 3.

$$S_\mu(n) = \begin{cases} 1 & \textit{if } n = 1 \\ 0 & \textit{if } n > 0 \end{cases}$$

Proof.

$$S_\mu(1) = \sum_{d \mid 1} \mu(d) = \mu(1) = 1$$

By multiplicativity, it suffices to prove $S_\mu(p^n) = 0\ \forall p, n$.

$$\begin{aligned} S_\mu(p^n) &= \sum_{d \mid p^n} \mu(d) \\ &= \sum_{i=0}^{n} \mu(p^i) \\ &= \mu(1) + \mu(p) + 0 + \dots + 0 \\ &= 0 \end{aligned}$$

☐

Theorem 5 (Möbius inversion formula)**.** *Let* $f : \mathbb{N} \to \mathbb{C}$*. Then*

$$f(n) = \sum_{d \mid n} \mu(d) S_f(\frac{n}{d}).$$

Proof.

$$\begin{aligned} \sum_{d \mid n} \mu(d) S_f\left(\frac{n}{d}\right) &= \sum_{d \mid n} \mu(d) \sum_{e \mid \frac{n}{d}} f(e) \\ &= \sum_{e \mid n} f(e) \sum_{\substack{d \mid n \\ s.t. e \mid \frac{n}{d}}} \mu(d) \\ &= \sum_{e \mid n} f(e) \underbrace{\sum_{d \mid \frac{n}{e} \mu(d)} = \begin{cases} 1 & \frac{n}{e} = 1 \\ 0 & \text{otherwise} \end{cases}}_{\text{Using } d \mid n \wedge e \mid \frac{n}{d} \Leftrightarrow ed \mid n \Leftrightarrow e \mid n \wedge d \mid \frac{n}{e} = f(n)} \end{aligned}$$

☐

0.5 Structure of $\mathbb{Z}_n^\times$

$$n = p_1^{\alpha_1} \dots p_l^{\alpha_l} \text{ with } p_i \neq p_j, i \neq j, \alpha_i \in \mathbb{N} \text{ where } p_i \text{ are primes}$$

From the CRT it follows that $\mathbb{Z}_n^\times \cong \mathbb{Z}_{p_1^{\alpha_1}}^\times \times \dots \times \mathbb{Z}_{p_l^{\alpha_l}}^\times$. So we only consider prime powers p^α, $p \in \mathbb{P}$, $\alpha \in \mathbb{N}$

0.5.1 Case 1: $\alpha = 1$

Theorem 6. *$\mathbb{Z}_p^\times$ is cyclic, i.e. $\mathbb{Z}_p^\times \cong \mathbb{Z}_{(p-1)}$*

Proof. Use structure theorem for finite abelian groups. If G is a finite abelian group then $\exists d_1, \dots d_l \in \mathbb{N}$ such that $1 < d_1 \mid d_2 \mid d_3 \mid \dots \mid d_l$, and $G \cong \mathbb{Z}_{d_1}^\times \times \dots \times \mathbb{Z}_{d_l}^\times$ thus, $\mathbb{Z}_p^\times \cong \mathbb{Z}_{d_1}^\times \times \dots \times \mathbb{Z}_{d_l}^\times$ (every element $x \in \mathbb{Z}_{d_1}^\times \times \dots \times \mathbb{Z}_{d_l}^\times$ satisfies $d_l x = 0 \Rightarrow$ every $x \in \mathbb{Z}_p^\times$ satisfies $x^{d_l} = 1$). $x^{d_l} - 1$ is a polynomial of degree d_l over the field $\mathbb{Z}_p \Rightarrow x^{d_l} - 1$ has $\leq d_l$ roots $\Rightarrow p - 1 \leq d_l$, but $p - 1 = d_1 \dots d_l \Rightarrow l = 1, p - 1 = d_l$ $\square$

Remark 9. *The same proof shows: Let F be a field, $G \leq F^\times$, $|G| < \infty$. Then G is cyclic.*

0.5.2 Case 2: $\alpha \geq 2$; $p \geq 3$

Denote $|x|$ as the order of x in $\mathbb{Z}_{p^\alpha}^\times$; i.e. $|x| = \min\{l \in \mathbb{N} : x^l \equiv 1 \mod p^\alpha\}$

$\left|\mathbb{Z}_{p^\alpha}^\times\right| = \phi(p^\alpha) = p^{\alpha-1}(p-1)$, find $x, y \in \mathbb{Z}_{p^\alpha}^\times$ such that $|x| = p^{\alpha-1}$, $|y| = p - 1$ then $|xy| = |x||y| = p^{\alpha-1}(p-1)$, since $\gcd(|x|, |y|) = 1$

Lemma 4.

$$(1+p)^{p^{n-1}} \begin{cases} \equiv 1 & \mod p^n \\ \not\equiv 1 & \mod p^{n+1} \end{cases}$$

Proof. Proof by induction

$n = 1$ ✓

$n \to n + 1$

$$\begin{aligned}
(1+p)^{p^{n-1}} &= 1 + ap^n, p \nmid a \\
(1+p)^{p^n} &= (1 + ap^n)^p \\
&= 1 + pap^n + \sum_{i=2}^{p-1} \binom{p}{i} (ap^n)^i + (ap^n)^p
\end{aligned}$$

$$p^{np} \mid \bullet, \quad np \geq n+2, \quad (\text{or } p \geq 3), \quad p^{2n+1} \mid \bullet, \quad 2n+1 \geq n+2$$

$$p \mid \binom{p}{i} = \frac{p!}{i!(p-i)!}, 1 \leq i < p \Rightarrow (1+p)^{p^n} \equiv 1 + ap^{n+1} \pmod{p^{n+2}}, p \nmid a$$

$\square$

2× Lemma: $x = 1 + p$ satisfies $|x| = p^{\alpha-1}$, now find y.

1. $\exists z \in \mathbb{Z} : |\bar{z}| = p - 1$ is $\mathbb{Z}_p^\times$

2. let $l := |E|$ is $\mathbb{Z}_{p^\alpha}^\times$

3. Then $p^\alpha \mid z^l - 1 \Rightarrow z^l \equiv 1 \mod p$
4. $\Rightarrow p - 1 \mid l$.
5. Let $y := z^{\frac{l}{p-1}}$, then $|\bar{y}| = p - 1$.

We have proven: Theorem: $\mathbb{Z}_{p^\alpha}^\times$ is cyclic, i.e. $\mathbb{Z}_{p^\alpha}^\times \cong \mathbb{Z}_{p^{\alpha-1}(p-1)}$, if $p \geq 3, \alpha \geq 1$. $p = 2$: $\mathbb{Z}_{2^\alpha}^\times \cong \left\{0, \alpha = 1 \quad \mathbb{Z}_2, \alpha = 2 \quad \mathbb{Z}_2 \times \mathbb{Z}_{p^{\alpha-2}}, \alpha \geq 3\right\}$

Corollary 1. *Let $m \in \mathbb{N}$. Then $\mathbb{Z}_m^\times$ is cyclic iff m has one of the following forms:*

- $m = 2$
- $m = 4$
- $m = p^\alpha, p \geq 3, \alpha \in \mathbb{N}$
- $m = 2p^\alpha, p \geq 3, \alpha \in \mathbb{N}$

In these cases a generator of $\mathbb{Z}_m^\times$ is called *a primitive root modulo m*.