$\mathbf{D}_{\mathbf{M}}$ - 07 **MA-217 Discrete Mathematics / Jan-Apr 2007**
Lectures: Tuesday/Thursday 15:45–17:15; Lecture Hall-1, Department of Mathematics

6. Prime Residueclass Groups

6.1. Let $m > 1$ be an odd natural number. Information on the orders of special elements in the prime residueclass group $\mathrm{A}_m^\times$ provide information on the prime factors of m and sometimes also used to prove that m is prime, in particular, if sufficient information on the prime factorisation of $m-1$ is known. The following example (and their variants) are classical and were already known to LUCAS, LEHMER and many other number theorist use them.

a). (Fermat's test for prime numbers) Suppose that: for every prime divisor p of $m-1$, there exists a $n \in \mathbb{Z}$ such that $n^{m-1} \equiv 1 \pmod{m}$ and $n^{(m-1)/p} \not\equiv 1 \pmod{m}$. Show that m is a prime number. Moreover, if a natural number $n \in \mathbb{Z}$ satisfy these conditions simultaneusly, then n is a primitive residue modulo m.

b). Let $m-1 = ab$ with relatively prime natural numbers a and b. Suppose that: for every prime divisor p of a there exists a (dependent on p) $n \in \mathbb{Z}$ such that

$$n^{m-1} \equiv 1 \bmod m \quad \text{and} \quad \gcd(n^{\frac{m-1}{p}} - 1, m) = 1\,.$$

Then for every factor q of m show that $q \equiv 1 \pmod{a}$. (**Hint:** If q is prime and if there exists a natural number $n \in \mathbb{Z}$ such that $n \not\equiv 1 \pmod{m}$ and $n^b \equiv 1 \pmod{m}$, then $q-1$ is divisible by the prime factors of a which are not prime factors of b.) Moreover, show that if $a > b$, then m must be prime.

6.2. Let $p \geq 3$ be a prime number, $\alpha \in \mathbb{N}^*$ and $n \in \mathbb{Z}$ be a primitive residue modulo p. Then show that: **a).** n or $n(1+p)$ is a primitive root modulo p^α. **b).** $n^p(1+p)$ is a primitive root modulo p^α.

6.3. Let p be a prime number ≥ 3. For $n \in \mathbb{Z}$ with $n \equiv 1 \pmod{p}$ and arbitrary $\gamma \in \mathbb{N}$ show that $\mathrm{v}_p(n^{p^\gamma} - 1) = \gamma + \mathrm{v}_p(n-1)$. (**Hint:** Induction on γ.)

6.4. Let p be a prime number ≥ 3 and let $\alpha \in \mathbb{N}^*$, $q := p^\alpha$. Further, let $\psi^\times : \mathrm{A}_q^\times \to \mathrm{A}_p^\times$ be the canonical homomorphism. Then show that the map $x \mapsto (\psi^\times(x), x^{p-1})$ is an isomorphism of groups from $\mathrm{A}_q^\times$ onto $\mathrm{A}_p^\times \times \mathrm{A}_q^\times(p)$, where $\mathrm{A}_q^\times(p)$ the (isomorphic to $\mathrm{Z}_{q/p}$) *p–primary component* of $\mathrm{A}_q^\times$.

6.5. Let p be a prime number ≥ 3 and $\alpha \in \mathbb{N}^*$. For $n \in \mathbb{Z}$ with $p \not| a$, let $\nu_\alpha(n)$ denote the order of the residue class of n in $\mathrm{A}_q^\times$, $q := p^\alpha$. Then show that:

$$\nu_\alpha(n) = \nu_1(n) p^\beta\,, \quad \text{where} \quad \beta := \max\{0, \alpha - \mathrm{v}_p(n^{p-1} - 1)\}\,.$$

(**Hint:** Use the earlier two exericses.) If $\alpha \geq 2$, then n is a primitive residue modulo p^α if and only if n is a primitive residue modulo p and $n^{p-1} \not\equiv 1 \pmod{p^2}$. (**Hint:** Look for the prime numbers p (say $< 10^7$) with $2^{p-1} \equiv 1 \pmod{p^2}$ resp. $3^{p-1} \equiv 1 \pmod{p^2}$. They are very rare!.)

6.6. Prove the following generalization of the *theorem of Wilson*: For $m \in \mathbb{N}^*$, we have

$$\prod_{\substack{0 \leq n < m \\ \gcd(n,m)=1}} n \equiv \begin{cases} -1 \pmod{m}, & \text{if } \mathrm{A}_m^\times \text{ is cyclic}\,, \\ \ \ 1 \pmod{m} & \text{otherwise}\ . \end{cases}$$

6.7. For $m \in \mathbb{N}^*$, let $\mathrm{e}(m)$ denote the exponent of the group $\mathrm{A}_m^\times$.

a). Let $n, m \in \mathbb{N}^*$ be such that $\gcd(n,m) = 1$. Then $\mathrm{e}(nm) = \mathrm{lcm}(\mathrm{e}(n), \mathrm{e}(m))$.

b). Let $m = nn_1 \cdots n_r$ be the prime decomposition of $m \in \mathbb{N}^*$, where n is a power of 2 and the n_i are powers of r distinct odd prime divisors of m. Then show that $\mathrm{e}(m) = \mathrm{lcm}(\mathrm{e}(n), \varphi(n_1), \ldots, \varphi(n_r))$.

6.8. Show that $\mathrm{A}_{24}^{\times}$ is not isomorphic to any other prime residueclass group $\mathrm{A}_m^{\times}$, $m \neq 24$.

6.9. a). Let p be a prime number ≥ 3 and let $\alpha \in \mathbb{N}^*$. Further, let a be an integer which is not divisible by p. For $n \in \mathbb{N}^*$, let $d := \gcd(n, r)$ with $r := \varphi(p^\alpha) = p^{\alpha-1}(p-1)$. Show that the congruence $x^n \equiv a \bmod p^\alpha$ has a solution if and only if $a^{r/d} \equiv 1 \pmod{p^\alpha}$. Moreover, in this case the congruence has exactly d incongruent solutions. — For $n = 2$ and $\alpha = 1$, this is the Euler's criterion for quadratic residue.

b). How many solutions are there for the equation $x^n = x$ in A_m, $n \geq 2$, $m \in \mathbb{N}^*$?

6.10. Let p be a prime number and let $t \in \mathbb{N}^*$. For p consecutive integers $a_1, \ldots, a_p$, show that: $a_1^t + \cdots + a_p^t \equiv \begin{cases} 0 \pmod{p} & \text{if } t \nmid p-1\,, \\ -1 \pmod{p}, & \text{if } t \mid p-1\,. \end{cases}$ (**Hint:** The group $\mathrm{A}_p^{\times}$ is cyclic.)

6.11. Let $m \in \mathbb{N}^*$ and N be (may be empty) the set of the primitive residue classes in $\mathrm{A}_m^{\times}$. Then $\prod_{x \in N} x = 1$ except in the cases $m = 3, 4, 6$. (**Hint:** Use the following assertion: If A is a commutative ring with $1 \neq -1$ and if A has finitely many units, then $\sum_{\varepsilon \in A^\times} \varepsilon = 0$, since $A^\times$ can be decomposed into the 2–sets $\{\varepsilon, -\varepsilon\}$.)

6.12. (Gauss) Let p be a prime and let N be the set of primitive roots modulo p, i.e., in $\mathrm{A}_p^{\times}$. Then $\sum_{x \in N} x = \mu(p-1)$, where μ is the Möbius function. (**Hint:** Decompose $\mathrm{A}_p^{\times}$ in its primary components: $\mathrm{A}_p^{\times} = G_1 G_2 \cdots G_r$, and consider $N = N_1 N_2 \cdots N_r$, where N_i is the set of generating elements of G_i.) Further, if p is odd > 3, then the product of primitive roots modulo p is $\equiv 1 \pmod{p}$.

6.13. Let p be a prime number and let $\alpha \in \mathbb{N}^*$. Show that there exists infinitely many prime numbers of the form $np^\alpha + 1$, $n \in \mathbb{N}$. (**Hint:** For a proof consider the function $\mathbb{N} \to \mathbb{N}^*$ defined by $f(x) := x^{p^{\alpha-1}(p-1)} + x^{p^{\alpha-1}(p-2)} + \cdots + x^{p^{\alpha-1}} + 1$. Let $p_0, \ldots, p_r$ be prime numbers with $p_i \equiv 1 \pmod{p^\alpha}$. Let q be a prime factor of $f(m)$, where $m := pp_0 \cdots p_r$. Then $m^{p^\alpha} - 1 = (m^{p^{\alpha-1}} - 1) f(m)$ and hence $m^{p^\alpha} \equiv 1 \pmod{q}$. Further, $m^{p^{\alpha-1}} \not\equiv 1 \pmod{q}$, since otherwise $p \equiv f(m) \equiv 0 \pmod{q}$. It follows that p^α is an order of an element in $\mathrm{A}_q^{\times}$, and hence $q \equiv 1 \pmod{p^\alpha}$. Therefore $p_{r+1} := q$ is a new prime number $\equiv 1 \pmod{p^\alpha}$. — **Remark:** This proof also shows that: If $p \geq 3$, then there are infinitely many prime numbers of the form $n2p^\alpha + 1$, $n \in \mathbb{N}$. For example, there are infinitely many prime numbers of the form $6n + 1$.)

6.14. Every finite abelian group is isomorphic to a subgroup and to a residue class group of a prime residue class grooup. (**Hint:** Use the Exercise 6.13.)

6.15. (Prime-test) Let $m > 1$ be an odd integer. If m is prime, then $a^{m-1} \equiv 1 \pmod{m}$ for every relatively prime integer a to m (by Fermat's little theorem). Conversely, if the condition $a^{m-1} \equiv 1 \pmod{m}$ is fullfilled for one (or more) $a \in \mathbb{Z}$, then m is expected to be prime (with very high probablity). The following remarks show that one must be very careful to apply this prime-test.

a). An odd integer $m > 1$ is called a pseudo prime number if $2^{m-1} \equiv 1 \pmod{m}$. The smallest pseudo-prime number which is not prime is $341 = 11 \cdot 31$. (**Remark:** Pseudo-prime numbers are also called Chinese prime numbers, since 25 centuries ago Chinese mathematicians made (prime-test with $a = 2$) a claim that: *a natural number n is prime if and only if $n \mid 2^n - 2$*. This criterion is reliable for all integers $n \le 340$. Needless to say that our example 341 lays the conjecture to rest; this was discovered in 1819. It can be shown that there are infinitely many pseudo- primes, the smallest being 341, 561, 645 and 1105.)

b). If m is a pseudo-prime number, then $2^m - 1$ is a larger pseudo-prime. In particular, there infinitely many pseudo-prime numbers which are not prime numbers.

c). Every Mersenne-number $M_p = 2^p - 1$, p prime and every Fermat-number $F_n = 2^{2^n} + 1$, $n \in \mathbb{N}$, is a pseudo-prime number. (**Remark :** In 1963 it has been shown (in analogy with the *Dirichlet's theorem* on primes in arithmetic progression) that any arithmetic progression $an + b$ with $\gcd(a, b) = 1$ contains infinitely many pseudo-primes. These "false primes" are much rarer than actual primes, for instance, there are only 245 pseudo-primes smaller than one million, in comparison with 78492 primes. The first example of an even pseudo-prime, namely the number $161038 = 2 \cdot 73 \cdot 1103$ was found in 1950.)

d). An odd integer $m > 1$ is called a Carmichael– number if the exponent $\mathrm{e}(m)$ (see Exercise 6.7) of the prime residue class group modulo m is a proper divisor of $m-1$. Show that this is equivalent to : For every relatively prime integer a to m, we have $a^{m-1} \equiv 1 \pmod{m}$; neverthless m is not prime. Every Carmichael–number is the product of at least 3 distinct prime numbers. The smallest Carmichael–number $561 = 3 \cdot 11 \cdot 17$. The pseudo-prime number 341 is not a Carmichael-number, since $31 \not| 11^{341} - 11$, we have $11^{341} \not\equiv 11 \pmod{341}$.(**Remark :** These exceptional numbers are also called absolute pseudo-primes. R. C. Carmichael was the first (1909) to notice their existence.)

e). Let $n = p_1 p_2 \cdots p_r$ be a composite, square-free natural number, where p_i are distinct prime numbers. If $p_i - 1 \big| n - 1$ for all $i = 1, \ldots, r$, then n is a Carmichael- number. — (D. Shanks) If t is a positive integer such that $p_1 := 6t + 1$, $p_2 := 12t + 1$ and $p_3 := 18t + 1$ are prime numbers, then $m := p_1 p_2 p_3$ is a Carmichael-number. (**Remark :** The natural numbers $1729 = 7 \cdot 13 \cdot 19$, $6601 = 7 \cdot 23 \cdot 41$, $10585 = 5 \cdot 29 \cdot 73$ are Carmichael-numbers. It is widely believed that there are infinitely many Carmichael-numbers, but this conjecture remains unproven and there are just 43 of them less than one million.) The natural number $9091 \cdot 18181 \cdot 27271$ is a Carmichael- number. How many percent of the residue classes modulo this number are prime residues? (**Remark :** For a refined version of this test see : D. E. Knuth, *The Art of Computer Programming*, Vol. 2, 4.5.4 : Algorithm P.)

6.16. Let $m \in \mathbb{N}^*$ be a square-free natural number and let $a \in \mathbb{N}^*$. Show that the power-map $\mathrm{A}_m \to \mathrm{A}_m$, $x \mapsto x^a$ is bijective if and only if a and $\varphi(m)$ are relatively prime. Moreover, in this case the map $x \mapsto x^b$, where $b \in \mathbb{N}^*$ and $ab \equiv 1 \pmod{\varphi(m)}$ is the the inverse map of the map $x \mapsto x^a$. If m is not square- free, then there is no $a \in \mathbb{N}^*$, $a \ge 2$, such that the map $x \mapsto x^a$ is a bijective map. (**Remark :** One can apply the power- map in coding theory. (RSA–Codes due to R. Rivest, A. Shamir and L. Adleman. See also Exercise T6.2 for more details). Let $m = pq$ be two distinct big prime numbers p, q (of more than hundred digits) and let $a \in \mathbb{N}^*$ be a relatively prime to $\varphi(m) = (m + 1) - (p + q)$. Let the message be given through the integer $x \in \mathbb{N}$ with $0 \le x < m$, which is interpreted as an element of A_m (for longer messages one can use the blocks of numbers of the form as x). The number x will be sent to the number $y \in \mathbb{N}$ with $0 \le y < m$ and $y \equiv x^a \bmod m$. The decoding $x \equiv y^b \bmod m$ simply depends on the knowledge of $b \in \mathbb{N}$ with $ab \equiv 1 \pmod{\varphi(m)}$, and therefore on $\varphi(m)$, which require the knowledge of the prime factorisation $m = pq$. Note that m and a are known to a third party. The power map $\mathrm{A}_m \to \mathrm{A}_m$, $x \mapsto x^a$ is required to be less expensive and this can be achieved if one use one of the following method. Let $a = \sum_{i=0}^{r} b_i 2^i$ with $b_i \in \{0, 1\}$ be the dual-expansion of a. — Method 1 : Compute $x_i := x^{2^i}$, $i = 0, \ldots, r$, sucessively by using the squares $x_{i+1} = x_i^2$ and there by take x^a as the product of 1 with those x_i for which $b_i = 1$. — Method 2 : At the end of the sequence $x_{r+1}, \ldots, x_0$ contructed by $x_{r+1} := 1$, $x_i^2 = x_{i+1}^2 x^{b_i}$ for $i = r, \ldots, 0$, we have $x_0 = x^a$.)

Below one can see Class-Notes and (simple) test-exercises.

Class-Notes/Test-Exercises

T6.1. Let $m \in \mathbb{N}^*$. In this section we investigate the prime residue class group modulo m, that is, the unit group $\mathrm{A}_m^\times$ of the prime ring A_m of *charateristic* m. (Recall that the characteristic of a ring A is the *order* [1]) of 1_A in the additive group $(A, +)$ of A and is denoted by $\mathrm{Char}(A)$. If $n \in \mathbb{Z}\,\mathrm{Char}(A)$, then $na = 0$ for all $a \in A$. All subrings of a have the same characteristic, namely $\mathrm{Char}(A)$. For every ring $\mathbb{A}$, , there is a unique ring homomorphism $\chi_A : \mathbb{Z} \to A$ such that $n \mapsto n \cdot 1_A$. The kernal of the ring homomorphism χ_A is generated by $\mathrm{Char}(A)$, i.e., $\mathrm{Ker}(\chi_A) = \mathbb{Z}\,\mathrm{Char}(A)$.

1). (Prime rings) Let A be a ring. A prime ring of A is the smallest subring of A; it is the subring $\mathbb{Z} \cdot 1_A$ of all integer multiples of the multiplicative identity 1_A. If $a = \mathbb{Z} \cdot 1_A$, then A is a prime ring of itself and in this case we say that A is a prime ring. For example, the ring of integers $\mathbb{Z}$ is a prime ring.

a). *A ring A is a prime ring if and only if its additive group $(A, +)$ is a cyclic group. Inparticular, prime rings are commutative and have no proper subrings.*

b). (Structure of the prime rings) *Let A be a prime ring of charateristic m. Then*:

(1) *If $m > 0$, then*: $|A| = m$ *and* $A = \{n \cdot 1_A := 0 \leq n < m\}$. *Two elements $r \cdot 1_A,\ s \cdot 1_A \in A$ with $r, s \in \mathbb{Z}$ are equal if and only if $r \equiv s \pmod{m}$. An element $r \cdot 1_A \in A$ with $r \in \mathbb{Z}$ is a non-zero divisor if and only if it is a unit; this is exactly the case if and only if* $\gcd(r, m) = 1$.

(2) *If $m = 0$, then*: $A = \{n \cdot 1_A : n \in \mathbb{Z}\}$, *where the elements $n \cdot 1_A$ are distinct for distinct $n \in \mathbb{Z}$. Further, A is an integeral domain with exactly two units elements 1_A and -1_A.*

c). *The prime rings of rings of equal characteristic are canonically isomorphic. Inparticular, prime rings of equal characteristic are canonically isomorphic.* Therefore for every natural number $m \in \mathbb{N}^*$, we can choose the concrete modell $\mathrm{A}_m = \mathbb{Z}/\mathbb{Z}m$.

d). *For a prime ring A of characteristic $m > 0$, the following statements are equivalent*:

(i) *A is a field.* (ii) *A is an integral domain.* (iii) *m is a prime number.*

e). *Let A be a prime ring of characteristic $m > 0$. Then the order of the unit group $A^\times$ is $\varphi(m)$, where φ is the Euler's totient function.*

f). (Euler's theorem) *Let $m \in \mathbb{N}^*$ and let $a \in \mathbb{Z}$ with* $\gcd(a, m) = 1$. *Then*: $a^{\varphi(m)} \equiv 1 \pmod{m}$.

g). (Fermat's little theorem) *Let $p \in \mathbb{P}$ be a prime number and let $a \in \mathbb{Z}$ be such that $p \nmid a$. Then*: $a^{p-1} \equiv 1 \pmod{p}$.

2). (Unit group of a prime ring --- Prime redisue classes) For $r \in \mathbb{Z}$, let $\overline{r}$ denote the residue class of r in $\mathbb{Z}/\mathbb{Z}m$. Then: *$\overline{r}$ is a unit in the ring $\mathbb{Z}/\mathbb{Z}m$ if and only if* $\gcd(r, m) = 1$, i.e., *if r and m are relatively prime. Inparticular, we have* $\mathrm{Ord}\,\mathrm{A}_m^\times = \varphi(m)$, *where φ denote the Euler's totient function.* Therefore the units in $\mathbb{Z}/\mathbb{Z}m$ are called the prime residue classes modulo m and the unit group $(\mathbb{Z}/\mathbb{Z}m)^\times$ is called the prime residue class group modulo m. An integer $r \in \mathbb{Z}$ is called a prime residue modulo m if $\overline{r}$ is a prime residue class modulo m, i.e, if $\overline{r} \in (\mathbb{Z}/\mathbb{Z}m)^\times$.

3). *If d is a divisor of m, then there is a unique, surjective ring homomorphism $\mathrm{A}_m \to \mathrm{A}_d$ which induce a canonical group homomorphism $\mathrm{A}_m^\times \to \mathrm{A}_d^\times$ on unit groups which is also surjective.* (**Proof:**

[1]) Note that we define the notion of an order of an element in a group slightly different from the standard text books, which is in many ways more convenient to work with: Let G be an arbitrary group with neutral element e, $a \in G$ and let $\mathrm{H}(a)$ be the subgroup generated by a, i.e., $\mathrm{H}(a)$ is the smallest subgroup of G containing a, in fact $\mathrm{H}(a) = \{a^n \mid n \in \mathbb{Z}\}$. Then the order of a is defined by $\mathrm{Ord}(a) := \begin{cases} |\mathrm{H}(a)|, & \text{if } \mathrm{H}(a) \text{ is finite,} \\ 0, & \text{if } \mathrm{H}(a) \text{ is not finite.} \end{cases}$ *For every element $a \in G$, we have $a^n = e$ if and only if $n \in \mathbb{Z} \cdot \mathrm{Ord}(a)$. Inparticular, $a^{\mathrm{Ord}(a)} = e$ and if $\mathrm{Ord}(a) > 0$, then $\mathrm{Ord}(a)$ is the smallest natural number $n \in \mathbb{N}^*$ such that $a^n = e$. Moreover, if G is finite, then every element $a \in G$ has order* $\mathrm{Ord}(a) > 0$ *and* $\mathrm{Ord}(a)$ *divides* $\mathrm{Ord}(G)$, *inparticular,* $a^{\mathrm{Ord}(G)} = e$.

If $a \in \mathbb{Z}$ with $\gcd(a, d) = 1$ then there exists $r \in \mathbb{N}$ such that $\gcd(a + rd, m) = 1$; for example, the product of those prime factors of m, which are not prime factors of either a or d.)

4). For every decomposition $m = m_1 \cdots m_r$ of m into factors $m_i \in \mathbb{N}^*$, let $\mathrm{A}_m \to \mathrm{A}_{m_i}$ denote the canonical ring homohomorphism and let $\psi : \mathrm{A}_m \to \mathrm{A}_{m_1} \times \cdots \times \mathrm{A}_{m_r}$ be the ring homomorphism defined by $a \mapsto (\psi_1(a), \ldots, \psi_r(a))$. Then: *$\psi$ is bijective if and only if $m_1, \ldots, m_r$ are pairwise relatively prime, i.e., $\gcd(m_i, m_j) = 1$ for every $1 \leq i, j \leq r$, $i \neq j$.* (**Proof:** Since the rings under consideration are finite, ψ is bijective if and only if ψ is injective. The kernel of ψ is generated by $n := \operatorname{lcm}(m_1, \ldots, m_r)$, i.e., $\ker\psi = \mathbb{Z}n/\mathbb{Z}m$. Therefore ψ is injective if and only if $m = n$ or equivalently $m_1, \ldots, m_r$ are pairwise relatively prime.)

5). *Let $m_1, \ldots, m_r$ be pairwise relatively prime natural numbers in $\mathbb{N}^*$ and let $m := m_1 \cdots m_r$. Then the canonical group homomorphism $\mathrm{A}_m^\times \to \mathrm{A}_{m_1} \times \cdots \times \mathrm{A}_{m_r}^\times$ is an isomorphism of groups. In particular, $\varphi(m) = \varphi(m_1) \cdots \varphi(m_r)$*, i.e., *the Euler's totient function φ is multiplicative.* (**Proof:** The canonical ring homomorphism in (4) is bijective and hence induces a group isomorphism from the unit group $\mathrm{A}_m^\times$ onto the unit group of the product of rings which is nothing but the direct product of the unit groups $\mathrm{A}_{m_i}^\times$. — **Remark:** Let $m = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ be the canonical prime decomposition of m. Then for understanding the structure of the prime residue class group modulo m, it is enough to understand the structure of the prime residue class group modulo a power p^α of a prime number p.)

6). *Let p be a prime number. Then the prime residue class group $\mathrm{A}_p^\times$ modulo p is a cyclic group.* More generally, *if G is a finite subgroup of the multiplicative group $K^\times$ of a field K, then G is cyclic.*(**Remark:** The assumption that G is finite is very important. The multiplicative groups $\mathbb{C}^\times$ and $\mathbb{R}^\times$ are not cyclic, since they are uncountable. The multiplicative groups $\mathbb{Q}^\times$ is not cyclic, not even finitely generated (use the Fundamental Theorem of Arithmetic). It is also interesting to note that: *if the multiplicative grou $K^\times$ of a field is cyclic, then K must be a finite field.*)

7). Let $m \in \mathbb{N}^*$ and let $a \in \mathrm{A}_m^\times$. Let $\nu_m(a)$ denote the order of the element a in the group $\mathrm{A}_m^\times$. Then:

a). $a^r \equiv a^s \pmod{m}$ if and only if $r \equiv s \pmod{\nu_m(a)}$. **b).** $a^r \equiv 1 \pmod{m}$ if and only if $r \equiv 0 \pmod{\nu_m(a)}$. In particular, $\nu_m(a) \big| \varphi(m)$. **c).** If a, b be integers with $\gcd(a, m) = \gcd(b, m) = 1$ and $\gcd(\nu_m(a), \nu_m(b)) = 1$, then $\nu_m(ab) = \nu_m(a) \cdot \nu_m(b)$. **d).** The elements $1, a, a^2, \ldots, a^{\nu_m(a)-1}$ are incongruent modulo m. **e).** Show that m is prime if and only if $\nu_m(a) = m - 1$ for some $a \in \mathrm{A}_m^\times$. **f).** The element a is called a primitive prime residue class if it generates the group $\mathrm{A}_m^\times$, or equivalently, $\nu_m(a) = \varphi(m)$, i.e., $\mathrm{A}_m^\times = \{1, a, a^2, \ldots, a^{\varphi(m)-1}\}$. An integer $n \in \mathbb{Z}$ is called a primitive residue modulo m if its residue class modulo m is a primitive prime residue class. (**Remark:** A primitive residue modulo m is also called a primitive root modulo m. In this language, the primitive residue classes modulo m are the solutions of the pure equation $x^n = 1$. If a primitive residue modulo m exists, then each prime residue system modulo m can be expressed as a geometric progression. This gives a powerful tool that can be used in problems involving prime residue systems. Unfortunately, not all prime residue class groups $\mathrm{A}_m^\times$ have primitive roots. See 13) below for more precise assertion.)

a). Let x be an odd integer and let $\alpha \in \mathbb{N}$, $\alpha \geq 3$. Then $x^{\varphi(2^\alpha)/2} \equiv 1 \pmod{2^\alpha}$. In particular, there are no primitive roots modulo 2^α. (**Hint:** First prove the case $\alpha = 3$ and then prove the assertion by induction on α.)

b). Let $m \in \mathbb{N}^*$ and let $a \in \mathbb{Z}$ be relatively prime integer to m. For any integer $k \in \mathbb{Z}$, show that $\nu_m(a) = \nu_m(a)/\gcd(k, \nu_m(a))$. In particular, $\nu_m(a^k) = \nu_m(a)$ if and only if $\gcd(k, \nu_m(a)) = 1$.

c). Let p be an odd prime number and let d be a divisor of $p - 1$. Then in every prime residue system modulo p, i.e., in the group $\mathrm{A}_p^\times$, there are exactly $\varphi(d)$ elements a such that $\nu_m(a) = d$. In particular, there are exactly $\varphi(p) = p - 1$ primitive roots modulo p.

d). Let p be an odd prime number and let g be a primitive root modulo p. Show that $\nu_p(-g) = \begin{cases} \nu_p(g), & \text{if } p \equiv 1 \pmod{4}, \\ (p-1)/2, & \text{if } p \equiv 3 \pmod{4}. \end{cases}$. In particular, $-g$ is a primitive root modulo p if and only if $p \equiv 1 \pmod{4}$. Further, show that the even powers $g^2, g^4, \ldots, g^{p-1}$ are the quadratic residues modulo p and the odd powers $g, g^3, \ldots, g^{p-2}$ are the non-quadratic residues modulo p.

e). Let p be a prime number of the form $p = 2^n + 1$, $n > 1$. Show that 3 is a primitive root modulo p, i.e., $\nu_p(3) = p - 1$.

f). Let p be a prime number of the form $p = 4q + 1$, where q is an odd prime number. Show that 2 is a primitive root modulo p, i.e., $\nu_p(2) = p - 1$.

g). Let p be an odd prime number. Show that if g is a primitive root modulo p, then g is also a primitive root modulo p^α with $\alpha \in \mathbb{N}^*$ if and only if $g^{p-1} \not\equiv 1 \pmod{p^2}$. Further, show that there exists a primitive root g modulo p such that $g^{p-1} \not\equiv 1 \pmod{p^2}$. In particular, there exists at least one primitive root modulo p^α if $\alpha \geq 2$.

h). Show that 7 is a primitive root modulo $p = 71$. Find all primitive roots modulo 71. Further, find primitive roots modulo p^2 and modulo $2p^2$.

8). Let p be a prime number and let $\alpha \in \mathbb{N}^*$. For an integer $n \in \mathbb{Z}$ which is relatively prime to p, we put $\nu_\alpha(n) := \nu_{p^\alpha}(n) =$ the order of the residue class of n in the group $\mathrm{A}^\times_{p^\alpha}$. Then either $\nu_{\alpha+1}(n) = \nu_\alpha(n)$ or $\nu_{\alpha+1}(n) = \nu_\alpha(n)p$. (**Proof:** The canonical group homomorphism $\mathrm{A}^\times_{p^{\alpha+1}} \to \mathrm{A}^\times_{p^\alpha}$ is surjective and its kernel is of order p.)

9). *Let p be a prime number. If n is a primitive residue modulo p, then either n or $n+p$ is a primitive residue modulo p^2.* (**Proof:** We have $\nu_1(n) = \nu_1(n+p) = \varphi(p) = p-1$. Further, $\nu_2(n)$ is either $p-1$ or $(p-1)p$. It follows that n is a primitive residue modulo p^2 if and only if $n^{p-1} \not\equiv 1 \pmod{p^2}$ and by the cancelattion law in the prime residue class group, this is further equivalent to $n^p \not\equiv n \pmod{p^2}$. Analogously, for $n+p$. Now, if n is not a primitive residue modulo p^2, then $n^p \equiv n \pmod{p^2}$. By the Binomial theorem $(n+p)^p = \sum_{i=0}^{p} \binom{p}{i} n^{p-i} p^i \equiv n^p + pn^{p-1}p \equiv n^p \equiv n \not\equiv n+p \pmod{p^2}$. Therefore $n+p$ is a primitive residue modulo p^2.)

10). *Let p be a prime number and let $\alpha \in \mathbb{N}^*$; if $p = 2$, then assume that $\alpha \geq 2$. Further, let $n \in \mathbb{Z}$ be relatively prime to p. Then: if $\nu_{\alpha+1}(n) = \nu_\alpha(n)p$, then $\nu_{\alpha+2}(n) = \nu_{\alpha+1}(n)p$.* (**Proof:** Let $r := \nu_\alpha(n)$. Then $\nu_{\alpha+1}(n) = rp$. We consider $m := n^r - 1$. Then clearly, $m \equiv 0 \pmod{p^\alpha}$, but $m \not\equiv 0 \pmod{p^{\alpha+1}}$. Then, for $i \in \mathbb{N}$, $i \geq 3$, m^i is divisible by $p^{\alpha+2}$, since $i\alpha \geq \alpha + 2$. Therefore, modulo $p^{\alpha+2}$, we have: $n^{rp} = (1+m)^p = \sum_{i=0}^{p} \binom{p}{i} m^i \equiv 1 + pm + \binom{p}{2} m^2$. In the case $p = 2, \alpha \geq 2$, m^2 is also divisible by $p^{\alpha+2}$. If $p \geq 3$, then $\binom{p}{2} m^2$ is divisible by $pp^{2\alpha}$ and hence by $p^{\alpha+2}$. Therefore $n^{rp} \equiv 1 + pm \pmod{p^{\alpha+2}}$. Since pm is divisible by $p^{\alpha+1}$, but not by $p^{\alpha+2}$, it follows that $n^{rp} \not\equiv 1 \pmod{p^{\alpha+2}}$ and hence $\nu_{\alpha+2}(n) \neq rp = \nu_{\alpha+1}(n)$. Therefore $\nu_{\alpha+2}(n) = \nu_{\alpha+1}(n)p$.)

11). *Let p be a prime number ≥ 3 and let $\alpha \in \mathbb{N}^*$. Then:*

(1) $\mathrm{A}^\times_{p^\alpha}$ *is a cyclic group.* (2) *If $n \in \mathbb{Z}$ is a primitive residue p^2, then n is primitive residue modulo p^α.* (**Proof:** By 6) and 9) there exists a primitive residue modulo p and modulo p^2. Therefore it is enough to prove (2). Therefore, let $n \in \mathbb{Z}$ be a primitive residue modulo p^2. Then $\nu_2(n) = \nu_1(n)p$. Now, the assertion follows by induction on α and 10).)

12). *Let $\alpha \in \mathbb{N}^*$. Then:*

(1) *If $\alpha \leq 2$, then $\mathrm{A}^\times_{2^\alpha}$ is a cyclic group.*

(2) *If $\alpha \geq 3$, then $\mathrm{A}^\times_{2^\alpha}$ is not cyclic. Moreover, it is a direct product of two cyclic groups one of order 2 and the other of order $2^{\alpha-2}$ which are generated by the residue classes of -1 and 5 modulo 2^α, respectively.* (**Proof:** For $\alpha \leq 3$ the assertions can be verified directly. Since $\nu_3(5) = 2\nu_2(5)$, it follows by induction on α and 10) that $\nu_\alpha(5) = 2^{\alpha-2}$ for all $\alpha \geq 2$. If $\alpha \geq 3$, then the residue class of -1 does not belong to the subgroup generated by the residue class of 5, since this is not true modulo 8. This proves the assertion.)

13). (Gauss) *Let $m \in \mathbb{N}^*$. The prime residue class group $\mathrm{A}^\times_m$ modulo m is cyclic if and only if m is of the form 1, 2, 4, p^α, $2p^\alpha$, where p is an arbitrary odd prime number and $\alpha \in \mathbb{N}^*$ is arbitrary.* (**Proof:** Let $p \geq 3$ be a prime number and let $\alpha \in \mathbb{N}^*$. Then $\varphi(p^\alpha) = (p-1)p^{\alpha-1}$ is an even number and hence it follows that there is an element in the group $\mathrm{A}^\times_{p^\alpha}$ of order 2. Let $m \in \mathbb{N}^*$ be such that $\mathrm{A}^\times_m$ is cyclic. Then there are at most one element of order 2 in the cyclic group $\mathrm{A}^\times_m$. Threrfore, in a direct decomposition of $\mathrm{A}^\times_m$ given in 5) corresponding to the canonical prime decomposition of m, there is only one factor of even order. Now, from 12) it follows that m must of the form given in the theorem. Conversely, if m is of the form given in the theorem, then it follows that the prime residue class group $\mathrm{A}^\times_m$ modulo m is cyclic by 11) and the remark: If $m = 2n$ with n odd, then $\mathrm{A}^\times_m \cong \mathrm{A}^\times_n$ by 5).)

14). Let $m \in \mathbb{N}^*$. Suppose that g is a primitive root modulo m. Then there are exactly $\varphi(\varphi(m))$ incongruent primitive roots modulo m. Moreover, the set $S = \{g^n \mid \gcd(n, \varphi(m)) = 1, 1 \leq n \leq \varphi(m)\}$ is the set of all primitive roots modulo m.

15). Let $m \in \mathbb{N}^*$ be a natural number which is not of the form $1, 2, 4, p^\alpha$ or $p^{2\alpha}$, where p is an odd prime number. Then for any relatively prime integer a, we have $a^{\varphi(m)/2} \equiv 1 \pmod{m}$.

16). (Index calculus) Let $m \in \mathbb{N}^*$. Suppose that g is a primitive root modulo m. Then $\mathrm{A}_m^\times = \{1, g, g^2, \ldots, g^{\varphi(m)-1}\}$. For each $a \in \mathbb{Z}$ which is relatively prime to m, there exists an unique integer k with $0 \leq k \leq \varphi(m)-1$ such that $a \equiv g^k \pmod{m}$. This integer k is called the index of a to the base $g \pmod{m}$ and we write $k = \mathrm{ind}_g(a)$. The following properties of indices are analogous to those of logarithms.

a). If $\gcd(a,m) = \gcd(b,m) = 1$, then $\mathrm{ind}_g(ab) = \mathrm{ind}_g(a) + \mathrm{ind}_g(b)$.

b). If $n \in \mathbb{N}^*$, then $\mathrm{ind}_g(a^n) \equiv n \cdot \mathrm{ind}_g(a) \pmod{\varphi(m)}$.

c). $\mathrm{ind}_g(1) = 0$ and $\mathrm{ind}_g(g) = 1$.

d). If $m > 2$, then $\mathrm{ind}_g(-1) = \varphi(m)/2$.

e). If g' is another primitive root modulo m, then $\mathrm{ind}_g(a) \equiv \mathrm{ind}_{g'}(a) \cdot \mathrm{ind}_g(g') \pmod{\varphi(m)}$.

17). The following examples illustrate the use of indices in solving congruences. Let $m \in \mathbb{N}^*$ be such that there is a primitive root g modulo m and let $a, b \in \mathbb{Z}$ be integers each of which is relatively prime to m. Then

a). (Linear Congruences) The linear congruence $ax \equiv b \pmod{m}$ is equivalent to the linear congruence $\mathrm{ind}_g(a) + \mathrm{ind}_g(x) \equiv \mathrm{ind}_g(b) \pmod{\varphi(m)}$.

b). (Binomial Congruences) The binomial congruence $x^n \equiv b \pmod{m}$ is equivalent to the linear congruence $n \cdot \mathrm{ind}_g(x) \equiv \mathrm{ind}_g(a) \pmod{\varphi(m)}$. Therefore, if $d = \gcd(\mathrm{ind}_g(a), \varphi(m))$, then the above linear congruence has a solution if and only if $d \big| \mathrm{ind}_g(a)$; moreover, in this case there are exactly d solutions. For example, the binomial congruence $x^8 \equiv a \pmod{17}$, the corresponding index congruence is $8\mathrm{ind}_3(x) \equiv \mathrm{ind}_3(a) \pmod{16}$. Since $d = \gcd(8, 16) = 8$ and $1, 16$ are the only residues mod 17 whose index is divisible by 8. In fact $\mathrm{ind}_3(1) = 0$ and $\mathrm{ind}_3(16) = 8$. Therefore the above congruence has no solutions if $a \not\equiv 1 \pmod{17}$ or $a \not\equiv 16 \pmod{17}$. For $a = 1$, the index congruence is $8\mathrm{ind}_3(x) \equiv 0 \pmod{16}$ and for $a = 16$, the index congruence is $8\mathrm{ind}_3(x) \equiv 8 \pmod{16}$. Each of these has exactly eight solutions modulo 16, namely those x whose ind_3 is even: $x \equiv 1, 2, 4, 8, 9, 13, 15, 16 \pmod{17}$ and those x whose ind_3 is odd; $x \equiv, 10, 11, 12, 14 \pmod{17}$, respectively.

c). (Exponential Congruences) The exponential congruence $a^x \equiv b \pmod{m}$ is equivalent to the linear congruence $x \cdot \mathrm{ind}_g(a) \equiv \mathrm{ind}_g(b) \pmod{\varphi(m)}$. Therefore, if $d = \gcd(\mathrm{ind}_g(a), \varphi(m))$, then the above linear congruence has a solution if and only if $d \big| \mathrm{ind}_g(b)$; moreover, in this case there are exactly d solutions. For example, the exponential congruence $25^x \equiv 17 \pmod{47}$, we have $\mathrm{ind}_5(25) = 2$, $\mathrm{ind}_5(17) = 16$ and $d = \gcd(2, 46) = 2$ and hence this congruence becomes $2x \equiv 16 \pmod{46}$ which has two solutions $x \equiv 8$ and $31 \pmod{46}$.. These are also solutions of the original exponential congruence $\pmod{47}$.

T6.2. (Cryptography) Classically, the making and breaking the secrete codes has been confined to diplomatic and military practices. With the growing quantity of digital data stored and communicated by eletronic-data processing systems, organizations in both the public and commercial sectors have felt the need to protect information from unwanted intrusion. Indeed, the widespread use of electronic funds transfers has made privacy a pressing concern in most financial transactions. Therefore, there has been a recent surge of interest by mathematicians and computer scientists in *cryptography* (from the Greek *kryptos* meaning *hidden* and *graphein* meaaning to *write*) — the science of making communications unitelligible to all except authorized parties. Cryptography is the only known practical means for protecting information transmitted through public communications networks, such as those using telephone lines, microwaves or satellites.

In the language of cryptography, where codes are called ciphers, the information to be concealed is called plaintext. After the transformation to a secret form, a message is called ciphertext. The process of converting from plaintest to ciphertext is called encrypting or enciphering, while the reverse process of changing from ciphertext back to palintext is called decrypting or deciphering.

One of the earliest cryptographic systems was used by the great Roman emperor JULIUS CAESAR around 50 B C. Carsar using a rudimentary subsitution cipher in which each letter of the alphabest is replaced by the letter which occurs three palces down the alphabet with the last three letters cycled back to the first three letters. For example, the plaintext message CAESAR WAS GREAT is transformed into the ciphertext FDHVDU ZDV JUHDV.

The Caesar cipher can be described easily by using congruences. Any plaintest is first expressed numerically by translating the characters of the text into digits by means of the bijection:

$\{A, B, C, \ldots, X, Y, Z\} \to \{01, 02, 03, \ldots, 24, 25, 26\}, \quad A \mapsto 01, \ldots, Z \mapsto 26$.

If P is digital equivalent to a plaintext letter and if C is the digital equivalent to the corresponding ciphertext letter, then $C \equiv P+3 \pmod{26}$,. Therefore, for instance, the letters of the above message are converted to their equivalents: 03 01 05 19 01 18 23 01 19 07 18 05 01 20 and using the congruence $C \equiv P+3 \pmod{26}$, this becomes the ciphertext 06 04 08 22 04 21 26 04 22 10 21 08 04 23 . Now to recover the palintext, the procedure is simply reversed by means of the congruence: $P \equiv C-3 \equiv C+23 \pmod{26}$.

The Caesar cipher is very simple and hence extremely insecure. Caesar himself soon abandoned this scheme, not only because of its insecurity, but also because of he didnot trust CIECERO, with whom he necessarily shared the secret of the cipher.

In conventional cryptographic systems, such as Caesar's cipher, the sender and receiver jointly have a secret *key*. The sender uses the key to encrypt the plaintext to be sent, while the receiver uses the same key in order to decrypt the ciphertext obtained. *Public-Key* crptography differs from the conventional cryptography in that it uses two keys, an encryption key and a decryption key. Although the two keys effect inverse operations and therefore related, there is no easily computed method of deriving the decryption key from the encryption key. Therefore the encryption key can be made public without compromising the decryption key; each user can encrypt messages, but only the intended recipient (whose decryption key id kept secret) can decipher them. A major advantage of the public-key cryptosytem is that it is unnecessary for each sender and receiver to exchange a key in advance of their decision to communicate with each other.

In 1977, R. RIVEST, A. SHAMIR and L. ADLEMAN proposed a publci cryptosystem which uses only elementary ideas from number theory. Their enciphering system is called RSA after the initials of the algorithm's inventors. Its security depends on the assumption that in the current state of computer technology, the factorization of the composite numbers with large prime factors is prohibitively time-consuming.

Each user fo the RSA system chooses a pair of distinct prime numbers p and q large enough that the factorization of their product $m = pq$ called the enciphering modulus, is beyind all current computational capabilities. For instance, one might pick p and q with 200 digits each, so that m has roughly 400 digits. Having selected m, the user then chooses a random positive integer a called the enciphering exponent, satisfying $\gcd(a, \varphi(m)) = 1$. the pair (m, a) is placed in a public file, analogous to a telephone directory, as the user's personal encryption key. This will allow anyone else in the communication network to encrypt and send a message to that individual. Notice that while m is openly revealed, the listed public-key does not mention the factors p and q of m.

The encryption process begins with the conversion of the message to be sent into x by means of a digital alphabet in which each letter, number or punctuation mark of the plaintext is replaced by two digit integer. It is assumed that the plaintext number $x < m$, where m is ciphering modulus; otherwise it would be impossible to distinguish x from any larger integer congruent to it modulo m. If meaasge is too long to be handled as a single integer $x < m$, then x can be broken into blocks of digits $x_1, \ldots, x_r$ of the appropriate size. Each block would be excrypted separately.

Looking up the intended recipient's encryption key (m, a) in the public directory, the sender disguises the plaintext number x as a ciphertext number y by raising x to the a-th power and then reducing the result modulo m.

At the other end, the authorised recipient deciphers the transmitted information by first determining the integer b, the secret recovery exponent, for which $ab \equiv 1 \pmod{\varphi(m)}$. Since $\gcd(a, \varphi(m)) = 1$, this linear congruence has a unique solution modulo $\varphi(m)$. in fact, $b \equiv a^{\varphi(\varphi(m))-1} \pmod{\varphi(m)}$; indeed, $ab \equiv a^{\varphi(\varphi(m))} \equiv 1 \pmod{\varphi(m)}$ by Euler's theorem. The recovery exponent can only be calculated by someone who knows both a and $\varphi(m) = (p-1)(q-1)$, and hence knows the prime factors p and q of m. Therefore b is secure from an illegitimate third party whose knowledge is limited to the public-key (m, a).

Matters have been arranged so that the recipients can now retrieve x from y by simply calculating y^b modulo m. Since $ab \equiv 1 + \varphi(m)t$ for some integer t, it follows that $y^b \equiv (x^a)^b \equiv x^{1+\varphi(m)t} \equiv x \cdot 1^t \equiv x \pmod{m}$, whenever $\gcd(x, m) = 1$. the assumption that $\gcd(x, m) = 1$ was made in order to use Euler's theorem. In the unlikely event that x and m are not relatively prime, a similar argument establishes that $y^b \equiv x \pmod{p}$ and $y^b \equiv x \pmod{q}$, which then yields the desired congruence $y^b \equiv x \pmod{m}$.

The major advantage of this ingenious procedure is that the encryption of a message does not require the knowledge of the two primes p and q, but only their product m; there is no need for any one other than receiver of the message ever to know the prime factors critical to the decryption process and for the present it appears to be quite safe.

For the RSA cryptosystem to be secure it must not be computationally fesible to recover the plaintext x from the information assumed to be known to a third party; namely listed public-key (m, a). The direct method to attack would be to attempt to factor m an integer of huge magnitude, for once the factors are determined, the recovery exponent b can be calculated from $\varphi(m) = (p-1)(q-1)$ and a. Our confidence in the RSA system rests on what is known as the *work factor*, — the expected amount of computer time needed to factor the product of two large primes. Factoring computationally more difficult than distinguishing between primes and composites. On today's fastest computer, a 200-digit number can routinely be tested for primality in less than 10 minutes, whereas the running time required to factor a composite number of the same size is prohibitive. It has been estimated that the quickest factoring algorithm known can use approximately $(1.2)10^23$ computer operations to resolve an integer with 200 digits into its prime factors, assuming that each operation takes one microsecond (10^{-6} seconds), then the factorization time would be about $(3.8)10^9$ years. Given unlimited computing time and some unimaginably efficient factoring algorithm, the RSA cryptosystem could be broken, but for the present it appears to be quite safe.

1). a). A linear cipher is defined by the congruence $C \equiv aP + b \pmod{26}$, where a and b are integers with $\gcd(a, 26) = 1$. Show that the corresponding decrypting congruence is $P \equiv a'(C - b) \pmod{26}$, where the integer a' satisfies $aa' \equiv 1 \pmod{26}$.

b). Using the cipher $C = 5P + 11 \pmod{26}$, encrypt the message NUMBER THEORY IS EASY.

c). Decrypt the message TZSVIW JQBVMIJ HL MVOOVI which was produced by the linear cipher $C \equiv 3P + 7$.

2). Let p and q be distinct prime nunmbers. If $m = pq = 274279$ and $\varphi(m) = 272376$, find primes p and q. (**Hint:** $p + q = m - \varphi(m) + 1$ and $p - q = \big((p+q)^2 - 4m\big)^{1/2}$. — (**Ans:** 1747 and 157).)

3). When RSA system is based on the public-key $(m, a) = (3233, 37)$, what is the recovery exponent for the cryptosystem? (**Ans:** 253.)

4). Encrypt the message GOLD MEDAL using the RSA algorithm with public-key $(m, a) = (2419, 3)$. (**Ans:** 2318 1932 1106 2197 1631 0337 1728.)

5). The ciphertext message produced by the RSA algorithm with public-key $(m, a) = (1643, 223)$ is 1451 0103 1263 0560 0127 0897 determine the original plaintext message. (**Hint:** The recovery exponent is $b = 7$. — (**Ans:** REPLY NOW.)

6). The ciphertext message produced by the RSA algorithm with public-key $(m, a) = (2419, 211)$ is 1037 0431 0629 0690 0204 2267 0595 determine the original plaintext message. (**Hint:** The recovery exponent is $b = 11$. — (**Ans:** SELL SHORT)

T6.3. (Latin Squares) Let N be a finite set with n elements. A map $f : N \times N \to N$ is called a Latin square (of order n over N) if for every $a \in N$, on the a–th "row" $\{a\} \times N$ and on the a–th "column" $N \times \{a\}$ the maps $f|\{a\} \times N$ and $f|N \times \{a\}$ by f are bijective. Two Latin squares f, g over N are called orthogonal, if the map $(f, g) : N \times N \to N \times N$ defined by $(x, y) \mapsto (f(x, y), g(x, y))$ is bijective. Let A denote a commutative ring.

a). Let $x_0, a, b \in A$. The affine function $f : A \times A \to A$ defined by $(x, y) \mapsto x_0 + ax + by$ is a Latin square (over A) if and only if a and b are units in A.

b). Two affine functions $f, g : A \times A \to A$ with $f(x, y) = x_0 + ax + by$ resp. $g(x, y) = y_0 + cx + dy$ are orthogonal Latin square if and only if a, b, c, d, $ad - bc \in A^\times$. (In the matrix notation the affine map (f, g) of $A \times A$ is the map $\begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} x_0 \\ y_0 \end{pmatrix} + \mathfrak{A} \begin{pmatrix} x \\ y \end{pmatrix}$, $\mathfrak{A} := \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbb{M}_2(A)$ and $\operatorname{Det} \mathfrak{A} := ad - bc$ is the determinant of $\mathfrak{A}$.)

c). A *Matrix* $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbb{M}_2(A)$ is called hyper-regular, if $a,\ b,\ c,\ d$ and $ad-bc$ are units A . Let $\mathrm{m}(A)$ denote the number of hyper-regular matrices with coeeficients in A . Then $\mathrm{m}(A) = |A^\times|^3 \widetilde{\mathrm{m}}(A)$, where $\widetilde{\mathrm{m}}(A)$ denote the number of units a in A such that $a - 1$ also a unit A . If A_1, A_2 are two finite commutative rings, then $\mathrm{m}(A_1 \times A_2) = \mathrm{m}(A_1)\mathrm{m}(A_2)$. If A is a field with q elements, then $\mathrm{m}(A) = (q-1)^3(q-2)$. Further, $\mathrm{m}(\mathrm{A}_n) = n^4 \prod_{\substack{p \text{ prime} \\ p|n}} \Bigl(1 - \frac{1}{p}\Bigr)^3 \Bigl(1 - \frac{2}{p}\Bigr)$. If $|A| \equiv 2 \pmod 4$, then $\mathrm{m}(A) = 0$. If $|A|$ is odd, then $\mathrm{m}(A) \neq 0$.

d). If $n \in \mathbb{N}^*$ and $n \not\equiv 2 \pmod 4$, then there exists a commutative ring A with n elements and $\mathrm{m}(A) \neq 0$. (This is trivial if one use the exitense of *Galois fields*, i.e., fields with q elements, where $q > 1$ is an arbitrary power of a prime number is used. In particular, for every natural number $n \in \mathbb{N}^*$ such that $n \not\equiv 2 \pmod 4$, there exists a orthogonal Latin squares of order n . (Remark: Euler conjectured that for $n \equiv 2 \pmod 4$ there are no orthogonal Latin squares of order n . For $n = 2$ this is clear. For $n = 6$ — Euler himself handled this case in the Euler's officers problem, 36 officers of 6 ranks and from 6 regiments in a square formation of size 6 by 6 . Each row and each column of this formation are to contain one and only one officer of each rank and one and only one officer from each regiment. We may lable the ranks and the regiments from 1 through 6 and assign to each officer a 2 sample of the integers 1, through 6 . The first componentof the 2-sample designates the officier's rank and the scond his regiment. Euler's problem then reduces to the construction of a pair of orthogonal Latin suqares of order 6 . Euler conjectured in 1782 that there exists no pair of orthogonal Latin squares of order $n \equiv 2 \pmod 4$ .Tarry around 1900 verified by a systematic enumeration the validity of Euler's conjecture for $n = 6$. But only recently the combined efforts of Bose, Shrikhande and Parker culminated in the following theoerem: *For all n with $n \equiv 2 \pmod 4$ and $n \neq 2, 6$, there exists a pair of orthogonal Latin squares of order n .* This theorem shows that the opposite of the expected state of affairs holds and illustrates the danger of leaping to general conclusions from limited empirical evidence. We cannot go into the intricacies of the proof of this theorem.

e). Let $\mathrm{M}(A)$ be the supremm of the numbers k such that there exist the affine functions $f_1, \ldots, f_k : A \times A \to A$ such that for all i, j with $i \neq j$ the functions $f_i,\ f_j$ are orthogonal Latin squares. $\mathrm{M}(A)$ is the supremum of the numbers k such that there exist units $a_1, \ldots, a_k$ in $A^\times$ such that the differences $a_i - a_j$ for $i \neq j$ are also units in A . Then $\mathrm{M}(A_1 \times A_2) = \mathrm{Min}\{\mathrm{M}(A_1), \mathrm{M}(A_2)\}$ for two finite commutative rings A_1, A_2 . If $A \neq 0$, then $\mathrm{M}(A) \leq |A| - 1$. Further, $\mathrm{M}(A) = |A| - 1$ if and only if A is a field. If A is a commutative ring with n elements, then $\mathrm{M}(A) \leq \mathrm{Inf}\{p^{\mathrm{v}_p(n)} - 1 \mid p \text{ prime}\,,\ p|n\}$. This inequality is an equality if $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$, for example, for the product ring $K_1 \times \cdots \times K_r$, where K_i is a field with $p_i^{\alpha_i}$ elements. Further, $\mathrm{M}(A_n) = \mathrm{Inf}\{p - 1 \mid p \text{ prime},\ p|n\}$.

f). Let $n \in \mathbb{N}^*$ and $N := \{0, \ldots, n-1\}$. If $f, g : N \times N \to N$ are orthogonal Latin squares, then

$$\begin{pmatrix} f(0,0)n + g(0,0)\,, & \ldots, & f(0,n-1)n + g(0,n-1) \\ \cdots\cdots & \cdots\cdots & \cdots\cdots \\ f(n-1,0)n + g(n-1,0)\,, & \ldots, & f(n-1,n-1)n + g(n-1,n-1) \end{pmatrix}$$

is a magic square of the numbers $0, \ldots, n^2-1$, i.e., the sum of the numbers in each row and in each column is $(n/2)(n^2-1)$. One can construct a magic square for $n = 12$. One can construct a magic square for $n = 12$. Already Adam Ries constructed a magic square corresponding to an odd natural number n essentailly by using a pair of affine functions $f, g : \mathrm{A}_n \times \mathrm{A}_n \to \mathrm{A}_n$, i.e., corresponding to the hyper-regular matrix $\begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}$. (**Remark:** We would like to mention the following often used method for the construction of orthogonal Latin square and hence that of magic squares: Let G be a finite group with neutral element. e . For every permutation $\varphi : G \to G$, the map $G \times G \to G$ defined by $(x, y) \mapsto x\varphi(y)$ is a Latin square. The Latin squares $(x, y) \mapsto x\varphi(y)$ resp. $(x, y) \mapsto x\psi(y)$ corresponding to the permutations $\varphi, \psi \in \mathfrak{S}(G)$ are orthogonal if and only if $y \mapsto (\varphi(y))^{-1}\psi(y)$ is a permutation of G . If φ and ψ are automorphisms of G , then the Latin squares corresponding to φ and ψ are orthogonal if and only if $\varphi(y) = \psi(y)$ only for $y = e$. In particular, the Latin squares corresponding to the automorphisms $\varphi := \mathrm{id}_G$ and ψ are orthogonal if and only if ψ has no fixed point other than the neutral element e,.)