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

7. Quadratic Residues — The Quadratic Reciprocity Law[1])

7.1. Let $\mathrm{M}_p = 2^p - 1$ be the Mersenne number corresponding to a prime number p .

a). (Fermat/Euler) If q is a prime divisor of M_p , then show that $q \equiv 1 \pmod{2p}$ and that $q \equiv \pm 1 \pmod 8$.

b). (Euler) Assume that $q := 2p+1$ is also prime. Show that if $p \equiv 3 \pmod 4$, then q divides M_p . In partisular, in this case M_p is not prime, if $p \geq 11$. (For example, 23 divides M_{11} ; 47 divides M_{23} ; 167 divides M_{83} .) Further show that if $p \equiv 1 \pmod 4$, then q does not divide M_p .

7.2. Let $\mathrm{F}_t = 2^r + 1,\ r := 2^t,\ t \geq 1$ be the Fermat number.

a). (Euler) Let p be a prime divisor of the Fermat number F_t , $t \geq 2$. Show that p is of the form $2^{t+2}n + 1$ with $n \geq 1$. (**Hint:** Show that 2 is a quadratic residue mod p and compute the order of the residue class $2 \pmod p$.) Further, show that F_5 is not prime.

b). (Pépin) Show that a Fermat number $\mathrm{F} := \mathrm{F}_t$ is prime if and only if $3^{(\mathrm{F}-1)/2} \equiv -1 \pmod{\mathrm{F}}$. In particular, if F is prime, then 3 is primitive residue modulo F . (**Hint:** If F is prime then consider $\mathrm{F} \equiv 2 \pmod 3$ and apply the Quadratic Reciprocity Law. For the converse consider the residue class of 3 in the prime residue class group mod F . — **Remark:** With this *Pépin test* for Fermat numbers it is easily checked that, for instance, $\mathrm{F}_5, \mathrm{F}_6, \mathrm{F}_7, \mathrm{F}_8, \mathrm{F}_9, \mathrm{F}_{10}$ are not prime; 641 is a factor of F_5 . However,, in general, it is difficult to find a non-trivial factor of a large Fermat number F_t , even when Pépin test shows that F_t is not a prime.)

[1]) The present section is devoted to a major contribution of GAUSS — *The Quadratic Reciprocity Law*. For those who consider the theory of numbers "The Queen of mathematics" this is one the jewels in her crown. The intrinsic beauty of the Quadratic reciprocity Law has long exerted a strange fascination for mathematicians. This was first stated (in a full generality) in a complicated form by EULER during the period 1744-1746 : *q is a quadratic residue mod p if and only if one of $\pm p$ is a residue mod $4q$* . In 1783 (the year of Euler's death) a second version appeared in his *Opuscula Analytica* : *$(a)^{(p-1)/2}p$ is a quadratic residue mod q if and only if q is a quadratic residue mod p* . LEGENDRE introduced his symbol in an article in 1785 and the same time stated the reciprocity law without using the symbol. He gave the elegant second formulation in his book in 1798. EULER gave a faulty proof, in a second paper in 1783, of a special case of the theorem. LEGENDRE gave a proof, but with a gap in it, in 1785. At the age of eighteen, Gauss (in 1795) rediscovered (apparently unaware of the work of either EULER or LEGENDRE) the Quadratic Reciprocity Law and after a year's unremitting labor in 1796, obtained the first complete proof; he wrote, "for the whole year this theorem tormented me and absorbed my best efforts until at last I obtained a proof." He published this (a difficult induction) and a second proof five years later in *Disquisitiones Arithmeticae*." — which was publised in 1801, although finished in 1798. GAUSS attributed the Quadratic Reciprocity Law to himself, taking the view that a theorem belongs to the one who gives the first rigorous demonstration. The indigent LEGENDRE was led to complain: "This excessive impudence is unbelievable in a man who has sufficient personal merit not to have the need of appropriating the discoveries of others." LEGENDRE regarded GAUSS as an enemy from that time on. All discussion of priority between the two was futile; since each clung to the correctness of his position, neither took heed of the other. GAUSS went on to publish five different demonstrations of what he called "the gem of higher arithmetic," while another was found among his papers. Apparently neither of LEGENDRE and GAUSS were aware of either of the general statements given by EULER — rather astonishing, considering that they both knew of his 1783 faulty proof and that the two 1783 papers were published in the same volume! Long before any general results were knownm FERMAT had characterized the primes of which 2 , -2 3 and -3 are reisdues; proofs were supplied by EUKER for ± 3 in 1760 and by LAGRANGE for ± 2 in 1775.

7.3. Let p be an odd prime number.

a). Let $q := 2p+1$. Then

(1) Assume that $p \equiv 1 \pmod 4$. Show that q is prime if and only if $2^p \equiv -1 \pmod{q}$. Moreover, in this case 2 is a primitive residue mod q and -2 is a quadratic residue mod q .

(2) Assume that $p \equiv 3 \pmod 4$. Show that q is prime if and only if $2^p \equiv 1 \pmod{q}$. Moreover, in this case -2 is a primitive residue mod q and 2 is a quadratic residue mod q .

b). Let p be an odd prime number and let $q := 4p+1$. Show that q is prime if and only if $4^p \equiv -1 \pmod{q}$. Moreover, in this case 2 and -2 are primitive residue mod q .

7.4. Let t , n be positive integers with $n+1 < 2^{t+2}$ and let $m = 2^t n + 1$. Further, let a be an integer such that the Jacobi–Symbol $\left(\frac{a}{m}\right) = -1$. Show that m is prime if and only if $a^{(m-1)/2} \equiv -1 \pmod{m}$. If $t \geq 2$ and if m and n are not divisible by 3 , then one can use the above test with $a = 3$.

7.5. Let $a \in \mathbb{Z}$ be an integer which is not a square (in $\mathbb{Z}$). Show that there exists infinitely odd prime numbers p such that $\left(\frac{a}{p}\right) = -1$. (**Hint:** We may assume that a has an odd prime factor q . Let c be an integer with $\left(\frac{c}{p}\right) = -1$. If $p_1, \ldots, p_r$ are odd prime numbers with $\left(\frac{a}{p_i}\right) = -1$, then we can find one more an odd prime number of this kind which is a factor of the natural number b , which satisfty the congruences $b \equiv 1 \bmod 8p_1 \cdots p_r \frac{a}{q}$ and $b \equiv c \bmod q$. — **Remark:** One can also formulate this result as: *Let* $a \in \mathbb{Z}$. *If the quadratic congruence* $x^2 \equiv a \pmod{p}$ *has a solution for al most all prime numbers, then* a *is a square in* $\mathbb{Z}$.)

7.6. Let $f(X) \in \mathbb{Q}[X]$ be a polynomial which takes integer values on integers and let $a, b \in \mathbb{Z}$. Let p be an odd prime number. Show that

a). If $\gcd(a,p) = 1$, then $\displaystyle\sum_{x \in \mathbb{Z}_p} \left(\frac{f(ax+b)}{p}\right) = \sum_{x \in \mathbb{Z}_p} \left(\frac{f(x)}{p}\right)$.

b). $\displaystyle\sum_{x \in \mathbb{Z}_p} \left(\frac{f(ax)}{p}\right) = \left(\frac{a}{p}\right) \sum_{x \in \mathbb{Z}_p} \left(\frac{f(x)}{p}\right)$.

c). If $\gcd(a,p) = 1$, then $\displaystyle\sum_{x \in \mathbb{Z}_p} \left(\frac{ax+b}{p}\right) = 0$.

d). If $\gcd(a,p) = \gcd(b,p) = 1$ and $f(x) = x(ax+b)$, then

$$\sum_{x \in \mathbb{Z}_p^\times} \left(\frac{f(x)}{p}\right) = \sum_{x \in \mathbb{Z}_p^\times} \left(\frac{a+bx}{p}\right) = -\left(\frac{a}{p}\right).$$

7.7. Let p be an odd prime number. Let $\varepsilon, \varepsilon' \in \{\pm 1\}$ and let $\mathrm{N}(\varepsilon, \varepsilon')$ denote the number of elements $x \in \{1, 2, \ldots, p-2\}$ such that $\left(\frac{x}{p}\right) = 1$ and $\left(\frac{x}{p}\right) = -1$. Then show that

a). $\displaystyle 4 \cdot \mathrm{N}(\varepsilon, \varepsilon') = \sum_{x=1}^{p-2} \left(1 + \varepsilon\left(\frac{x}{p}\right)\right) \cdot \left(1 + \varepsilon'\left(\frac{x+1}{p}\right)\right)$.

b). $4 \cdot \mathrm{N}(\varepsilon, \varepsilon') = p - 2 - \varepsilon' - \varepsilon\varepsilon' - \varepsilon\left(\frac{-1}{p}\right)$. In particular, $\mathrm{N}(1,1) = \frac{p-4-\left(\frac{-1}{p}\right)}{4}$, $\mathrm{N}(-1,-1) = \mathrm{N}(-1,1) = \frac{p-2-\left(\frac{-1}{p}\right)}{4}$ and $\mathrm{N}(1,-1) = 1 + \mathrm{N}(1,1)$. (**Hint:** Use part a).)

c). For every prime number p, show that there exists integers (x, y) such that $x^2 + y^2 = 1 \equiv (\bmod\ \mathrm{p})$. (**Hint:** Use part b).)

7.8. Let p be an odd prime number. Show that:

a). If $p \equiv 1 \pmod 4$, then $\sum_{a=1}^{p-1} a\big(\frac{a}{p}\big) = 0$.

b). If $p \equiv 1 \pmod 4$, then $\displaystyle\sum_{a=1\,;\,\left(\frac{a}{p}\right)=1}^{p-1} a = \frac{p(p-1)}{4}$.

c). If $p \equiv 3 \pmod 4$, then $\sum_{a=1}^{p-1} a^2\big(\frac{a}{p}\big) = p\sum_{a=1}^{p-1} a\big(\frac{a}{p}\big)$.

d). If $p \equiv 1 \pmod 4$, then $\sum_{a=1}^{p-1} a^3\big(\frac{a}{p}\big) = \frac{3}{2}p\sum_{a=1}^{p-1} a^2\big(\frac{a}{p}\big)$.

e). If $p \equiv 3 \pmod 4$, then $\sum_{a=1}^{p-1} a^4\big(\frac{a}{p}\big) = 2p\sum_{a=1}^{p-1} a^3\big(\frac{a}{p}\big) - p^2\sum_{a=1}^{p-1} a^2\big(\frac{a}{p}\big)$.

7.9. et p be an odd prime number with $p \equiv 1 \pmod 4$ and let $t := (p-1)/2$.

a). Prove that $\Big(1-2\big(\frac{2}{p}\big)\Big)\sum_{a=1}^{t} a\big(\frac{a}{p}\big) = p\cdot\frac{1-\left(\frac{2}{p}\right)}{2}\sum_{a=1}^{t}\big(\frac{a}{p}\big)$. (**Hint:** If a runs through the numbers $\{1, 2, \ldots, t\}$, then a and $p-a$ (respectively, $2a$ and $p-2a$) together run through the numbers $\{1, 2, \ldots, p-1\}$.)

b). Prove that $\Big(\big(\frac{2}{p}\big)-2\Big)\sum_{a=1}^{p-1} a\big(\frac{a}{p}\big) = p\sum_{a=1}^{t}\big(\frac{a}{p}\big)$.

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

Class-Notes/Test-Exercises

T7.1. Let p be an odd prime number and let $a \in \mathbb{Z}$ be an integer with $a \not\equiv 0 \pmod p$, i.e., $\gcd(a, p) = 1$ or equivalently, $a \in \mathbb{Z}_p^\times$.

1). (Quadratic residues mod p) If the congruence $x^2 \equiv a \pmod{\mathrm{p}}$ has a solution, then a is called a quadratic residue mod p. Otherwise, a is called a non- quadratic residue mod p. Note that if $b \in \mathbb{Z}$ with $a \equiv b \pmod{\mathrm{p}}$, then a is a quadratic residue mod p if and only if b is a quadratic residue mod p. Therefore for determining whether a is a quadratic residue mod p or not, we may assume that $0 < a < p$.

2). (Euler's Criterion) EULER devised a simple criterion for deciding whether an integer a is a quadratic residue modulo a given prime number p: *Let $a \in \mathbb{Z}$ and let p be an odd prime number with $gcd(a, p) = 1$. Then a is a quadratic residue mod p if and only if $a^{(p-1)/2} \equiv 1 \pmod p$*

3). (Solutions of quadratic congruences) Let p be an odd prime and let $a \not\equiv 0 \pmod p$, i.e., $\gcd(a, p) = 1$. Consider the quadratic congruence $ax^2 + bx + c \equiv 0 \pmod p$. Since p is odd, $\gcd(4a, p) = 1$ and hence the above congruence is equivalent to $(2ax + b)^2 - (b^2 - 4ac) = 4a(ax^2 + bx + c) \equiv 0 \pmod p$. Now put $y = 2ax + b$ and $d = b^2 - 4ac$ to get $y^2 \equiv d \pmod p$. If $x \equiv x_0 \pmod p$ is a solution of the original congruence, then $y \equiv 2ax_0 + b \pmod p$ is the solution of the last qudratic congruence. Conversely, if $y \equiv y_0 \pmod p$ is a solution of the last quadratic congruence, then the linear congruence $2ax \equiv y_0 - b \pmod p$ can be solved to obtain a solution of the original quadratic congruence. Therefore the problem of finding a solution to a quadratic congruence is equivalent to that of finding a solution to a linear congruence and a quadratic congruence of the form $x^2 \equiv a \pmod p$. If $p|a$, then $x \equiv \pmod p$ is the only solution of $x^2 \equiv a \pmod p$. Therefore to avoid trivialties assume that $p \nmid a$. Note that of $x^2 \equiv a \pmod p$ admits a solution $x = x_0$, then there is also a second solution $x = p - x_0$ and this solution is not congruent to the first one, since $x_0 \equiv \pmod p$, then $2x_0 \equiv 0 \pmod p$, or equivalently (since p is odd) $x_0 \equiv 0 \pmod p$

which is not possible (since $a \not\equiv 0 \,(\mathrm{mod}\, p)$). These two solution exhaust the incongruent solutions of $x^2 \equiv a \,(\mathrm{mod}\, p)$ by *Lagrange's theorem* [2]). In short: *The quadratic congrunce* $x^2 \equiv a \,(\mathrm{mod}\, p)$ *has exactly two solutions or no solution.* The folloiwng two basic problems dominate the theory of quadratic residues: (1) Given a prime number p, determine which integers $n \in \mathbb{Z}$ are quadratic residues mod p and which are not quadratic residues mod p. (2) Given an integer $n \in \mathbb{Z}$, determine those prime numbers p for which n is a quadratic residues mod p and hose prime numbers p for which n is not a quadratic residues mod p.

a). Show that the quadratic equation $6x^2 + 5x + 1 = 0$ has no solution in the integers, but the quadratic congruence $6x^2 + 5x + 1 \equiv 0 \,(\mathrm{mod}\, p)$ has a solution for every prim number p. Find the solutions of the quadratic congruences $3x^2 + 9x + 7 \equiv 0 \pmod{13}$ and $5x^2 + 6x + 1 \equiv 0 \pmod{23}$.

b). Show that the quadratic residue mod p are congruent modulo p to the integers $1^2, 2^2, \ldots, \dfrac{(p-1)}{2}^2$. What are the quadratic residues mod 17 ? Is 3 a quadratic residue mod 23 and mod 31 ?

c). Suppose that a is a quadratic residue mod p. Show that: (1) a is not a primitive root mod p, i.e., a is not a generator of the cyclic group $\mathbb{Z}_p^\times$. (2) $p - a$ is a quadratic residue mod p if and only if $p \equiv 1 \,(\mathrm{mod}\, 4)$. (3) If $p \equiv 3 \pmod 4$, then $x \equiv \pm a^{(p+1)/4} \pmod{\mathrm{p}}$ are the solutions of the quadratic congruence $x^2 \equiv a \pmod{\mathrm{p}}$.

d). Suppose that $p \equiv 1 \pmod 8$ and that a is a primitive root mod p. Show that the solutions of the quadratic congruence $x^2 \equiv 2 \pmod{\mathrm{p}}$ are given by $x \equiv \pm(a^{7(p-1)/8} + a^{(p-1)/8} \pmod{\mathrm{p}}$. (**Hint:** First prove that $(a^{3(p-1)/8} \equiv -1 \pmod{\mathrm{p}}$.) Use this to find all solutions of the quadratic congruences $x^2 \equiv 2 \pmod{17}$ and $x^2 \equiv 2 \pmod{41}$.

e). Suppose that a is quadratic residue mod p. If $b, c \in \mathbb{Z}$ are two integers with $bc \equiv a \pmod{\mathrm{p}}$, then show that either both b and c are quadratic residues mod p or both b and c are non-quadratic residues mod p.

f). Let $b \in \mathbb{Z}$ be an integer such that either both a and b are quadratic residues mod p or both a and b are non-quadratic residues mod p. Show that the quadratic congruence $ax^2 \equiv b \pmod{\mathrm{p}}$ has a solution. (**Hint:** Let $a' \in \mathbb{Z}$ be such that $aa' \equiv 1 \pmod{\mathrm{p}}$. Multiply the gice congruence by a'.)

g). Let $b \in \mathbb{Z}$ be an integer with $b \not\equiv 0 \,(\mathrm{mod}\, p)$. Prove that either all the three of the quadratic congruences $x^2 \equiv a \pmod{\mathrm{p}}$, $x^2 \equiv b \pmod{\mathrm{p}}$, $x^2 \equiv ab \pmod{\mathrm{p}}$ have solutions or exactly one of them admits a solution.

T7.2. (Legendre–Symbol and its properties) Let p be an odd prime number. For an integer $a \in \mathbb{Z}$, the Legendre–Symbol $\left(\frac{a}{p}\right)$ is defined by:

$$\left(\frac{a}{p}\right) = \begin{cases} 0, & \text{if } p|a\,, \\ 1, & \text{if } p \not| a \text{ and if } a \text{ is a quadratic residue mod } p\,, \\ 1, & \text{if } p \not| a \text{ and if } a \text{ is not a quadratic residue mod } p\,, \end{cases} \quad .$$

1). Let p be an odd pirme number and let $a, b \in \mathbb{Z}$ be integers with $\gcd(a, p) = \gcd(b, p) = 1$. Then: **a).** $\left(\frac{1}{p}\right) = 1$. **b).** If $a \equiv b \pmod{\mathrm{p}}$, then $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$. **c).** $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$. **d).** (Euler's Criterion) $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{\mathrm{p}}$. In particular, $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$. **e).** $\left(\frac{a^2}{p}\right) = 1$ and $\left(\frac{a^2 b}{p}\right) = \left(\frac{b}{p}\right)$.

2). Find the values of $\left(\frac{a}{p}\right)$ in each of the following cases: $a = -1, 2, -2, 3$ and $p = 11, 13, 17$. **3).** List all the solutions of each of the congruences: $x^2 \equiv a \pmod{11}$ and $x^2 \equiv a \pmod{11^2}$, where $a = 1, 3, 4, 5, 9$ (**Hint:** $1, 3, 4, 5, 9$ are precisely the quadratic residues mod 11.)

4). Which of the following congruences have solutions? How many?

(1) $x^2 \equiv 2 \pmod{59}$; $x^2 \equiv -2 \pmod{59}$; $x^2 \equiv -1 \pmod{59}$.

[2]) A theorem of LAGRANGE which deals with the number of solutions of a polynomial congruence: *Let p be a prim number and let $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$ with $a_n \not\equiv 0 \,(\mathrm{mod}\, p)$ be a polynomial of degree $n \geq 1$ with integer coefficients, then the polynomial congruence $f(x) \equiv 0 \,(\mathrm{mod}\, p)$ has at most n incongruent solutions modulo p.*

(2) (1) $x^2 \equiv 2 \pmod{61}$; $x^2 \equiv -2 \pmod{61}$; $x^2 \equiv -1 \pmod{61}$.

5). Let $p \geq 3$ be a prime number. Show that the equation $x^4 + 1 \equiv 0 \pmod{p}$ has a solution if and only if $p \equiv 1 \pmod{8}$ ist.

6). Compute the incongruent solutions for the following congruence equations : $x^2 \equiv 2 \pmod{134}$. $x^2 \equiv 2 \pmod{94}$. $x^2 \equiv -2 \pmod{268}$.

7). Does the equation $x^2 + 4x + 1 = 0$ have a solution in K_{47}? For which prime numbers p the equation $x^2 - x + 1 = 0$ has a solution in K_p ?

8). Let p be an odd prime number. Then $x^2 \equiv 2 \pmod{p}$ has solutions if and only if $p \equiv 1$ or $7 \pmod{8}$.

9). Let a, b, c be integers, $D := b^2 - 4ac$ and $p \geq 3$ be a prime number which does not divide a . Show that the quadratic equation $ax^2 + bx + c = 0$ has no solution resp. one resp. two solutions in K_p if and only if $\left(\frac{D}{p}\right)$ is equal to -1 resp. 0 resp. 1 .

10). Let a and b be relatively prime integers. For every odd prime divisor p of a resp. b , assume that b resp. a is a quadratic residue mod p . Further, assume that one of the integers a, b, ab is congruent to $1 \pmod{8}$. Show that the equation $(x^2 - a)(x^2 - b)(x^2 - ab) \equiv 0 \pmod{m}$ has a solution for every $m \in \mathbb{N}^*$ (See also T7.1-???).)

11). Let p be an odd prime number. Prove that the quadratic residues modulo p are congruent to $1^2, 2^2, \ldots, ((p-1)/2)^2$. Deduce that if $p > 3$ then the sum of the quadratic residues is divisible by p . Further, show that if $p \equiv 1 \pmod{4}$, then $\displaystyle\sum_{x \in \mathbb{Z}_p^\times \, ; \, \left(\frac{x}{p}\right) = 1} x = p(p-1)/4$.

12).

T7.3. (Quadratic Reciprocity Law)

T7.4. (Jacobi[3]) – Symbol [4]) and its properties) We shall extend the definition of Legendre–Symbol. Let a and b be integers.

(1) If a and b are not relatively prime, then we put $\left(\frac{a}{b}\right) := 0$. If $a \neq 0$, then we put $\left(\frac{a}{1}\right) = \left(\frac{a}{-1}\right) := 1$. In general we put $\left(\frac{a}{b}\right) = \left(\frac{a}{-b}\right)$.

(2) If now $b > 0$ and $b = p_1 \cdots p_r$ is the prime decomposition of b , where p_i are odd prime numbers ≥ 3 , then we define $\left(\frac{a}{b}\right) := \prod_{i=1}^r \left(\frac{a}{p_i}\right)$, where (a/p_i) is the ordinary Legendre–Symbol.

1). The following rules are immediate : For integers a, a' and odd integers b, b' , we have:

[3]) Carl Gustav Jacob Jacobi (1804-1851). Mathematics in Germany was at low ebb when Jacobi was a student at Potsdam and Berlin and he was mostly self-educated, through reading the works of Euler and Lagrange. He became a splendid teacher and did much to revive German mathematics in Königsberg and Berlin. His first love was the *theory of elliptic functions*, but he also wrote in other branches of *analysis* and in *geometry* and *mechanics*. Interested in the history of mathematics, Jacobi was a prime mover in the publication of Euler's collected work. He and Dirichlet were close friends; they independently sired two quite different kinds of analytic number theory. Although his friends predicted he would work himself to death, he died instead of smallpox.

[4]) Calculation with the Legendre–Symbol $\left(\frac{a}{p}\right)$ is hampered by the fact that a must be a prime number to use the Quadratic reciprocity Law. Therefore it was pointed out at the end of the proof of the Quadratic Reciprocity Law that it is necessary to have available rather extensive factorisation tables if one is to evaluate Legendre–Symbol with large entries. Partly to obviate such a list and partly for theoretical purposes, it has been found convenient to extend the definition of the Legendre–Symbol $\left(\frac{a}{b}\right)$ so as to give meaning to when b is not a prime number. Owing to this remark Jacobi extended the definition of Legendre–Symbol, this general Symbol is called the Jacobi– Symbol. We shall see that others of its properties are also similar to those of the Legendre–Symbol, but there is one crucial point at which the similarity breaks down: it may happen that $\left(\frac{a}{b}\right) = 1$ even when a is not a quadratic residue mod b . See ???.

(1) If $a \equiv a'$ (mod b), then $\left(\frac{a}{b}\right) = \left(\frac{a'}{b}\right)$. (2) $\left(\frac{aa'}{b}\right) = \left(\frac{a}{b}\right)\left(\frac{a'}{b}\right)$. (3) $\left(\frac{a}{bb'}\right) = \left(\frac{a}{b}\right)\left(\frac{a}{b'}\right)$. (4) If a is a quadratic residue mod b, then $\left(\frac{a}{b}\right) = 1$. (**Hint:** Note that b is odd by hypothesis. — **Remark:** The converse is not true, for example, $\left(\frac{2}{9}\right) = \left(\frac{2}{3}\right)\left(\frac{2}{3}\right) = (-1)(-1) = 1$, but 2 is not a quadratic residue mod 9.)

2). For every natural number b, we have $\left(\frac{-1}{b}\right) = (-1)^{\frac{b-1}{2}}$ and $\left(\frac{2}{b}\right) = (-1)^{\frac{b^2-1}{8}}$. (**Proof:** For the proof of the first formula, let $b = p_1 \cdots p_r$ be the prime factorisation of b and $t_i := (p_i - 1)/2$. Then $\left(\frac{-1}{b}\right) = \prod_{i=1}^r \left(\frac{-1}{p_i}\right) = \prod_{i=1}^r (-1)^{t_i} = (-1)^t$, where $t := \sum_{i=1}^r t_i$. It is enough to show that t and $(b-1)/2$ have the same parity. This is clear from the equality $(b-1)/2 = (\prod_i (2t_i + 1) - 1)/2$. The second formula can be proved similarly. •)

3). For relatively prime odd integers $a,\ b$ with $b \geq 3$, we have $\left(\frac{a}{b}\right)\left(\frac{b}{a}\right) = (-1)^{\frac{a-1}{2}\,\frac{b-1}{2}}$.

(**Proof:** First we consider the case $a > 0$. If $a = q_1 \cdots q_s$ is the prime factorisation of a and $u_j := (q_j - 1)/2,\ u := \sum_{j=1}^s u_j$, then $\left(\frac{a}{b}\right) = \prod_i \left(\frac{a}{p_i}\right) = \prod_{i,j} \left(\frac{q_j}{p_i}\right) = \prod_{i,j} \left(\left(\frac{p_i}{q_j}\right) \cdot (-1)^{t_i u_j}\right) = \left(\frac{b}{a}\right) \cdot (-1)^w$ with $w := \sum_{i,j} t_i u_j = \sum_j (\sum_i t_i) u_j = tu$. Now, it is enough to show that tu has the same parity as the product of $(a-1)/2$ and $(b-1)/2$. But this is clear, since we have already seen above that t has the same parity as $(b-1)/2$ and similarly u has the same parity as $(a-1)/2$. If $a < 0$, then $(a/b) = (-1/b)(-a/b)$ and use the already proved formulas. •)

4). Let $p \neq 3$ be a prime number and let $q := 2^t p + 1$ with $t \in \mathbb{N},\ 2 \leq t \leq 7$. Show that q is prime if and only if $3^s \equiv -1$ (mod q), where $s := 2^{t-1} p$. Moreover, in this case (except the case $p = 5$ and $t = 3$) 3 primitive residue mod q.

5). To each of the natural numbers $r = 1$ resp. 3 resp. 5 resp. 7 there exists infinitely many prime numbers p such that $p \equiv r$ (mod 8). (**Hint:** Consider the sequences of natural numbers of the form $m^4 + 1$ resp. $2m^2 + 1$ resp. $4m^2 + 1$ resp. $8m^2 - 1$.)

6). To each of the natural numbers $r = 1$ resp. 5 resp. 7 resp. 11 there exists infinitely many prime numbers p such that $p \equiv r$ (mod 12). (**Hint:** Consider the sequences of natural numbers of the form $m^4 - m^2 + 1$ resp. $4m^2 + 1$ resp. $4m^2 + 3$ resp. $12m^2 - 1$. In the first case, if $m \equiv 1$ (mod 12), then m^3 is an element of order 4 in the prime residue class group modulo every prime dividor of $m^4 - m^2 + 1$.)

7). Compute $(38\,115/121\,103)$ and $(3\,113\,113/3\,131\,313)$.

8). (In this exercise we need some elementary concepts about permutations) Let b be an odd integer, a be an arbitrary integer which is relatively prime to b and let λ_a denote the multiplication by a on the additive group $H := \mathbb{Z}/b\mathbb{Z}$. Then $\lambda_a : H \to H$ is an automorphism of H and hence λ_a is a permutation of the set H. Moreover, the signature of this permutation is: $\operatorname{Sign} \lambda_a = \left(\frac{a}{b}\right)$. (**Hint:** (Zolotarev/Frobenius 1872. — One can be content to start with the case $b = p$ a prime. It is enough to consider a primitive root z (mod p); show that the multiplication $\lambda_z : \mathbb{Z}_p^\times \to \mathbb{Z}_p^\times$ is a cycle of length $(p-1)$. — For a generalisation of this see P. Cartier, Sur une généralisation des symboles de Legendre–Jacobi, L'enseignement math. **16**, 31–48 (1970).)

T7.5. Let $p \neq q$ be odd prime numbers and let $q^* := (-1)^{(q-1)/2} q$. Then show that $\left(\frac{p}{q}\right) = \left(\frac{q^*}{p}\right)$.

T7.6. Let p be an odd prime number.

a). $(3/p) = 1$ if and only if $p \equiv \pm 1$ (mod 12).

b). $(-3/p) = 1$ if and only if $p \equiv 1$ (mod 6).

c). Describe the value of $(\pm 6/p)$ by using the residue class of p modulo 24.

T7.7. For solving quadratic equations modulo a odd prime numebr p, we fact the following basic problem: For $a \in \mathbb{Z}$ with $\left(\frac{a}{p}\right) = 1$, construct a $x \in \mathbb{Z}$ with $x^2 \equiv a$ (mod p).

a). If p is of the form $4n - 1$, then we may take $x = a^n$. If p is of the form $8n + 5$ and if i ia an integer with $i^2 \equiv -1$ (mod p), then we may take $x = a^{n+1}$, if $a^{2n+1} \equiv 1$ (mod p), and we may take $x = i a^{n+1}$, if $a^{2n+1} \equiv -1$ (mod p).

b). Compute a solution of the equation $x^2 + x + 1 \equiv 0$ (mod 637).

c). For an effective solution of the quadratic congruence equation one can obtain (due to Tonelli 1891): Let $p = 1 + 2^\alpha v$ with v odd and $\alpha \geq 1$. Let H be the subgroup of order 2^α of the prime residue class group modulo p . The power map $y \mapsto y^v$ maps the prime residue class group $\mathbb{Z}_p^\times$ onto the subgroup H . We are looking for an integer b with $\left(\frac{b}{p}\right) = -1$. Then the residue class of $c := b^v$ is a generator for H . For every element $h \in H$ one can efficiently compute n such that $h \equiv c^n \pmod{p}$. (If 2^s, $s \geq 1$, is the order of h , then the order of $hc^{-2^{\alpha-s}}$ is $\leq 2^{s-1}$.) Let d be uniquely determined by $dc \equiv 1 \pmod{p}$. — Now, if $a^v \equiv c^n \pmod{p}$, then $x := d^{n/2}a^{(v+1)/2}$ is an integer with $x^2 \equiv a \pmod{p}$.

d). Compute a solution of the equation $x^2 \equiv 2 \pmod{641}$.