21-373, Algebraic Structures, Department of Mathematical Sciences, Carnegie Mellon University
Fall 2011: (Math Studies Section) Monday, Wednesday, Friday, 10:30 am, Porter Hall 226B.
Luc Tartar, University Professor of Mathematics, Wean Hall 6212, tartar@cmu.edu

4- Wednesday September 7, 2011.

Definition 4.1: If G is a group and $a \in G$, then for $n > 0$ one writes a^n for $a \cdots a$ with n factors a, for $n < 0$ one writes $a^n = a^{-1} \cdots a^{-1}$ with $|n|$ factors a^{-1}, and one writes $a^0 = e$.

One says that a and b *commute* if $b\,a = a\,b$.

Remark 4.2: One checks easily that for all $m, n \in \mathbb{Z}$ and all $a \in G$ one has $a^m a^n = a^{m+n}$, and it means that the mapping $n \mapsto a^n$ is an homomorphism from $\mathbb{Z}$ into G.

If a commutes with b,[1] then a commutes with b^{-1}, since by multiplying $b\,a = a\,b$ on the left and on the right by b^{-1} gives $a\,b^{-1} = b^{-1}a$. If a commutes with b and c, then a commutes with $b\,c$ since $a\,(b\,c) = (a\,b)\,c = (b\,a)\,c = b\,(a\,c) = b\,(c\,a) = (b\,c)\,a$. One deduces that if a and b commute, then a^m commutes with b^n for all $m, n \in \mathbb{Z}$.

Definition 4.3: If G is a group, a subset $H \subset G$ is a *subgroup* of G if

i) $e \in H$
ii) for all $h_1, h_2 \in H$, one has $h_1 h_2 \in H$,
iii) for all $h \in H$, one has $h^{-1} \in H$,

and one writes $H \leq G$. A subgroup H of G is called *proper* if $H \neq G$, and it is called *non-trivial* if $H \neq \{e\}$.

Remark 4.4: It is equivalent to say that for $H \subset G$, H is a subgroup of G if[2]

a) $H \neq \emptyset$,
b) for all $h_1, h_2 \in H$, one has $h_1 h_2^{-1} \in H$.

Indeed, taking $h_2 = h_1 \in H$ gives $e \in H$, and then taking $h_1 = e$ shows that $h_2^{-1} \in H$, and then replacing h_2 by h_2^{-1} gives $h_1 h_2 \in H$.

The notation $\leq$ for subgroups is natural because it is an order relation.

Definition 4.5: For a subgroup H of G, a *left coset* of H in G is any subset of the form $a\,H = \{a\,h \mid h \in H\}$ for some $a \in G$, and a *right coset* of H in G is any subset of the form $H\,b = \{h\,b \mid h \in H\}$ for some $b \in G$. The *order* of H, written $|H|$, is its cardinality (i.e. its number of elements if H is finite), and the *index* of H, written $[G\!:\!H]$,[3] is the cardinality of the set of left cosets (equal to the cardinality of the set of right cosets).[4]

H is a *normal subgroup* of G if for all $g \in G$ one has $g\,H = H\,g$, or equivalently $g\,H\,g^{-1} = H$ for all $g \in G$, [5] and one writes $H \lhd G$.

Remark 4.6: Left cosets form a partition of G (and right cosets also form a partition of G), i.e. if $a\,H \cap b\,H \neq \emptyset$ then $a\,H = b\,H$:[6] indeed, $a\,h_1 = b\,h_2$ implies $b = a\,h_1 h_2^{-1}$, so that $b\,h = a\,h_1 h_2^{-1} h \in a\,H$ for all $a \in H$, implying $b\,H \subset a\,H$, and reversing the roles of a and b gives $a\,H \subset b\,H$.

In order to check that H is a normal subgroup of G, it is enough to show that $g\,H\,g^{-1} \subset H$ for all $g \in G$, because by multiplying by g^{-1} on the left and by g on the right, one deduces that $H \subset g^{-1} H\,g$ for all $g \in G$, and by replacing g by g^{-1} it is the same as $H \subset g\,H\,g^{-1}$ for all $g \in G$.

[1] The relation ‘commutes with’ in a group G is reflexive and symmetric, but it is not always transitive if G is non-Abelian.

[2] One should not forget a), since b) is true for the empty set $\emptyset$, because all propositions beginning by $\forall h \in H$ are true if $H = \emptyset$.

[3] In the case where a field F is an extension of a field E, the same notation $[F\!:\!E]$ is also used to denote the dimension of F over E. The context should then make clear which notation is used.

[4] There is a bijection from left cosets to right cosets, since the bijection $g \mapsto g^{-1}$ maps the left coset $a\,H$ onto the right coset $H\,a^{-1}$.

[5] One should notice that $a\,H = H\,a$ does not mean that a commutes with the elements of H, but that for $h \in H$ there exist $h_1, h_2 \in H$ such that $a\,h = h_1 a$ and $h\,a = a\,h_2$

[6] Said otherwise, if $a\,\mathcal{R}\,b$ means $b \in a\,H$, then $\mathcal{R}$ is an equivalence relation: reflexivity follows from $a = a\,e$, symmetry follows from $b = a\,h$ implying $a = b\,h^{-1}$, and transitivity follows from $b = a\,h_1$ and $c = b\,h_2$ implying $c = a\,(h_1 h_2)$.

The relation $\triangleleft$ is not always a transitive relation (hence not an order relation) in a non-Abelian group, i.e. $G_1 \triangleleft G_2 \triangleleft G_3$ and G_3 non-Abelian do not imply that G_1 is a normal subgroup of G_3,[7] but if G is an Abelian group, all its subgroups are normal subgroups.

Lemma 4.7: If f is an homomorphism from a group G_1 into a group G_2, then the image $f(G_1)$ is a subgroup of G_2 and the kernel of f (i.e. $H = f^{-1}(\{e_2\})$) is a normal subgroup of G_1.
Proof: Since $f(e_1) = e_2$, one has $e_2 \in f(G_1)$. If $a, b \in f(G_1)$, then $a = f(\alpha), b = f(\beta)$ for some $\alpha, \beta \in G_1$, so that $a\,b^{-1} = f(\alpha)f(\beta)^{-1} = f(\alpha)f(\beta^{-1}) = f(\alpha\,\beta^{-1}) \in f(G_1)$, hence $f(G_1)$ is a subgroup of G_2.

For $g \in G_1$ and $h \in H$ (i.e. $h \in G_1$ and $f(h) = e_2$) one has $f(g\,h\,g^{-1}) = f(g)\,f(h)\,f(g^{-1}) = f(g)\,e_2\,f(g)^{-1} = e_2$, so that $g\,H\,g^{-1} \subset H$, hence $H \triangleleft G_1$.

Definition 4.8: If $A \subset G$, the *subgroup generated by* A, denoted $\langle A\rangle$, is the smallest subgroup of G containing A. The *order* of an element $g \in G$ is the order of the subgroup $\langle g\rangle$ generated by g. A group G is *cyclic* if it is generated by one element element $a \in G$, i.e. $G = \langle a\rangle$, and each such a is then called a *generator* of G; a group G is *finitely generated* if $G = \langle A\rangle$ for a finite set A.

Remark 4.9: Because an intersection of subgroups of G is obviously a subgroup of G, $\langle A\rangle$ is just the intersection of all subgroups of G containing A (and there is at least G in the list); notice that $\langle\emptyset\rangle = \{e\}$. If $A \neq \emptyset$, then for each $a \in A$ all the terms a^n for $n \in \mathbb{Z}$ belong to $\langle A\rangle$, and then $\langle A\rangle$ contains the products of elements of this form, so that it contains $\{a_1^{k_1} \cdots a_m^{k_m} \mid m \geq 1, a_1, \ldots, a_m \in A, k_1, \ldots, k_m \in \mathbb{Z}\}$, and since this set is obviously a subgroup of G it is equal to $\langle A\rangle$. In particular, for each $g \in G$ one has $\langle g\rangle = \{g^n \mid n \in \mathbb{Z}\}$.

Either g has infinite order and $\langle g\rangle \simeq \mathbb{Z}$, or g has finite order so that $g^m = g^n$ for some $m \neq n$, hence $g^k = e$ for some $k \geq 1$; let d be the smallest positive integer with $g^d = e$, so that $\{g, \ldots, g^d = e\}$ has d distinct elements; for each $n \in \mathbb{Z}$, the Euclidean division gives $n = d\,q + r$ for a quotient $q \in \mathbb{Z}$ and a remainder $r \in \{0, \ldots, d-1\}$, and then $g^n = (g^d)^q g^r = g^r$, so that $\langle g\rangle = \{e, g, \ldots, g^{d-1}\}$. In particular d is the order of g, and $g^k = e$ implies that k is a multiple of d.

Lemma 4.10: The subgroups of $\mathbb{Z}$ have the form $m\,\mathbb{Z}$ for $m \in \mathbb{N}$, so that a subgroup H which is proper ($H \neq \mathbb{Z}$) and non-trivial ($H \neq \{0\}$) is made of the multiples of an integer $m \geq 2$.
Proof: If a subgroup H of $\mathbb{Z}$ is non-trivial, it contains a smallest positive element m, and for each $h \in H$, the Euclidean division gives $h = m\,q + r$ for a quotient $q \in \mathbb{Z}$ and a remainder $r \in \{0, \ldots, m-1\}$, but since $r \in H$ (because h and $m\,q$ belong to H) one deduces that $r = 0$ by the choice of m.

Remark 4.11: $\mathbb{Z}$ has a second operation, multiplication, which makes it a (commutative) *ring*, but it has special properties which are not shared by all rings,[8] and it took some time to discover which definitions to take for general rings; it is then useful to wonder if all the notions invented are really natural.

For groups, the notion of a normal subgroup is natural: on one hand it characterizes the kernels of homomorphisms (which are the natural mappings between groups), and on the other hand (as we shall see in another lecture) it is the right notion for having an operation on the left cosets (or right cosets) so that a *quotient group* can be defined. For rings, the kernel of an homomorphism is an *ideal*, and it is also related to defining a *quotient ring*, but $\mathbb{Z}$ is special because its ideals coincide with its subgroups.

$\mathbb{Z}$ has no *zero divisor*, i.e. non-zero elements a, b such that $a\,b = 0$, and since it is commutative it is an example of an *Integral Domain* (abbreviated ID).

In order to generalize the existence of the Euclidean division in $\mathbb{Z}$, one invented the notion of an *Euclidean domain.*

Since the ideals/subgroups of $\mathbb{Z}$ are generated by one element, one invented the notion of *principal ideal*, which are generated by one element (similar to the notion of cyclic groups for groups) and of *Principal Ideal Domain* (abbreviated PID), whose all ideals are principal. One then generalized the notion by defining a *Noetherian ring*,[9] whose all ideals are finitely generated, and all these notions will become more natural

[7] Counter-examples with G_1 not a normal subgroup of G_3 will be shown later in the course.

[8] In this course, all the rings will be assumed to be *unital*, i.e. have an identity for multiplication, denoted 1, which is different from 0, the identity for addition, which is denoted $+$.

[9] Max Noether, German mathematician, 1844–1921. He worked in Heidelberg and in Erlangen, Germany.

when one will consider polynomials with coefficients in general rings.[10]

Remark 4.12: In $\mathbb{N}$, a *prime* p is any integer ≥ 2 such that its only divisors are 1 and p (so that 1 is not considered a prime), but the general notion for rings gives $\pm p$ in the case of $\mathbb{Z}$, so that there is a particular choice which is made in deciding that primes are positive. This is due to the fact that a *unit* in a commutative ring is an element which has an inverse for multiplication, and that the units in $\mathbb{Z}$ are ± 1, and some general notions are only defined up to *associates* (and b is an associate of a means $b = a\,u$ for a unit u); however, one also needs to define an *irreducible* element in a general ring, and the notions of prime and irreducible coincide if the ring is a *Unique Factorization Domain* (abbreviated UFD), implied by being a PID.

It has been known since the ancient Greeks that every integer $n \geq 2$ has a unique factorization $n = p_1^{k_1} \cdots p_r^{k_r}$ where $p_1, \ldots, p_r$ are distinct primes (which one orders by $p_1 < p_2 < \ldots$, and this selection using the order relation cannot be done in a general UFD) and $k_1, \ldots, k_r \geq 1$. For two integers $m, n \geq 2$, using the distinct primes $p_1, \ldots, p_s$ appearing in their factorizations, one has $m = p_1^{\alpha_1} \cdots p_s^{\alpha_s}$ and $n = p_1^{\beta_1} \cdots p_s^{\beta_s}$ with $\alpha_i, \beta_i \geq 0$ and one of them ≥ 1 for $i = 1, \ldots, s$, and the *greatest common divisor* (abbreviated gcd) of m and n, denoted (m, n) is $d = p_1^{\gamma_1} \cdots p_s^{\gamma_s}$ with $\gamma_i = \min\{\alpha_i, \beta_i\}$ for $i = 1, \ldots, s$.

Since it is difficult to factorize large numbers,[11] it is useful to observe that there is a simple algorithm for computing the gcd of n_1 and n_2 with $n_1 > n_2 > 1$,[12] and LAMÉ has estimated the number of operations it may take,[13] and it involves the *Fibonacci sequence*,[14] which itself uses the *golden ratio* $\rho = \frac{1+\sqrt{5}}{2}$, and the number of steps is $\leq \frac{\log(n_2)}{\log(\rho)} + 4$.[15]

Definition 4.13: The *Euler function* φ is defined for $n \geq 1$ by $\varphi(n)$ equal to the number of integers $k \in \{1, \ldots, n\}$ which are *relatively prime* with n, i.e. with $(k, n) = 1$.

Remark 4.14: By looking at the algorithm for finding the gcd, one sees that if $d = (n_1, n_2)$ then there exist $\alpha, \beta \in \mathbb{Z}$ such that $d = \alpha\, n_1 + \beta\, n_2$ (Bachet's identity).[16] One deduces that for $n \geq 2$ and $a \neq 0$, the equation $a\,x + b = 0 \pmod{n}$ has a solution $x \in \mathbb{Z}$ if and only if b is a multiple of the gcd (a, n), and x is then defined modulo $\frac{n}{(a,n)}$. In particular, a has an inverse modulo n if and only if $(a, n) = 1$, so that $\varphi(n)$ is the number of units in the ring $\mathbb{Z}_n$.

[10] Why care about polynomials with coefficients in general rings? Even though one is interested in polynomials with coefficients in a field F like $\mathbb{Q}$, $\mathbb{R}$, or $\mathbb{C}$, one first observes that polynomials in one variable form a ring denoted $F[x]$ which is an Euclidean domain (since there is an Euclidean algorithm for polynomials with coefficients in a field), hence a PID, but the polynomials in two variables $F[x, y]$ is not a PID, and since one may consider it as $R[x]$ with $R = F[y]$, it is useful to discover a property that $R[x]$ inherits when R has it: being a UFD (unique factorization domain), or being a Noetherian ring are such properties.

[11] This difficulty is used in *public key cryptography*, like for the *RSA system*, named after RIVEST, Adi SHAMIR, and ADLEMAN: one sends messages in a "secure" way to a person by encrypting x as $y = x^d \pmod{n}$, and this person knows a value of e for decrypting by $x = y^e \pmod{n}$, and it works if $d\,e = 1 \pmod{\varphi(n)}$ by Euler's theorem (and x relatively prime with n). The RSA method chooses $n = p_1 p_2$ with two distinct large primes (about one hundred decimal digits nowadays) p_1, p_2, so that $\varphi(n) = (p_1 - 1)\,(p_2 - 1)$, and d must be chosen relatively prime with $\varphi(n)$. Although n is known, its factorization is kept secret, and the actual state of the art does not permit to find the factorization in a reasonable amount of time.

[12] The algorithm consists in first dividing n_1 by n_2, i.e. $n_1 = q_1 n_2 + n_3$ with $0 \leq n_3 < n_2$, then dividing n_2 by n_3, i.e. $n_2 = q_2 n_3 + n_4$ with $0 \leq n_4 < n_3$, and repeating this operation until $n_k = 0$, so that the gcd is n_{k-1} and the algorithm has used $k - 2$ steps.

[13] Gabriel LAMÉ, French mathematician, 1795–1870. He worked in St. Petersburg, Russia and in Paris, France. Lamé's system in linearized elasticity is named after him.

[14] It is defined by $F_0 = F_1 = 1$ and $F_n = F_{n-1} + F_{n-2}$ for all $n \geq 2$: since $n_{k-1} \geq 1 = F_1$ and $n_{k-2} \geq 2 = F_2$, one has $n_{k-3} \geq n_{k-2} + n_{k-1} \geq F_3$ (because $q_{k-3} \geq 1$), and by induction $n_2 \geq F_{k-2}$, which shows that if $F_{\ell+1} > n_2 \geq F_\ell$, the gcd is found after at most $\ell + 2$ steps of the algorithm (and if $n_1 = F_{\ell+1}$ and $n_2 = F_\ell$, one finds that $n_j = F_{\ell+2-j}$ for $j \leq \ell + 1$).

[15] Using $\rho^2 = \rho + 1$ and $\frac{1}{\rho} = \rho - 1 = \frac{\sqrt{5}-1}{2}$, one deduces that $F_n = a\,\rho^n + b\,\rho^{-n}$ if $a + b = 1$ and $a\,\rho + b\,\rho^{-1} = 1$, i.e. $a = \rho^{-2}, b = \rho^{-1}$, hence $F_n \geq \rho^{n-2}$ and the number of steps is $\leq \frac{\log(n_2)}{\log(\rho)} + 4$.

[16] Claude Gaspard BACHET, sieur de Méziriac, French mathematician, 1581–1638.

Theorem 4.15: (Fermat's theorem) If p is prime and a is not a multiple of p, then $a^{p-1} = 1 \pmod{p}$.

Theorem 4.16: (Euler's theorem) If $n \geq 2$ and a is relatively prime with n, then $a^{\varphi(n)} = 1 \pmod{n}$.

Remark 4.17: For p prime, one has $\varphi(p) = p - 1$, so that Euler's theorem is a generalization of Fermat's theorem. Since FERMAT did not give proofs of his statements, other mathematicians had to supply a written proof for everyone to be sure that his statements were correct; it was probably while he was seeking a proof of Fermat's theorem that EULER found a proof which implies the stronger statement.

Lagrange's theorem implies that in a finite group G every element $g \in G$ satisfies $g^{|G|} = e$, since the order d of g divides $|G|$, and from $g^d = e$ one takes the mth power with $m = \frac{|G|}{d}$ and one obtains $g^{|G|} = e$. If one observes that the units in a ring R form a multiplicative group, denoted R^*, Euler's theorem is the preceding observation for $G = \mathbb{Z}_n^*$, which has order $\varphi(n)$, and Fermat's theorem is the case where n is a prime p.

Lemma 4.18: For each d dividing n (with $n \geq 2$), $\mathbb{Z}_n$ has exactly $\varphi(d)$ elements of order d, so that $\sum_{d|n} \varphi(d) = n$. For each d dividing n, $\mathbb{Z}_n$ has exactly one subgroup of order d.
Proof: Since one deals with addition, one uses the additive notation.[17] An element a has order d if $d\,a$ is a multiple of n and no smaller integer than d has this property. Since d divides n, let $n = d\,\delta$, so that $a = k\,\delta$, and then $j\,a$ is a multiple of n if and only if $j\,k$ is a multiple of d, and the smallest such j is $\frac{d}{(k,d)}$, so that it is d if and only if $(k, d) = 1$, and there are $\varphi(d)$ such values for k. Since every integer $\in \{0, \ldots, n-1\}$ has an order which divides n, one deduces that $\sum_{d|n} \varphi(d) = n$.

Each element of order d generates a subgroup of order d, but all the $\varphi(d)$ such elements generates the same subgroup, because it is isomorphic to $\mathbb{Z}_d$, and $\mathbb{Z}_d$ has exactly $\varphi(d)$ generators.

Lemma 4.19: (Chinese remainder theorem) If $m_1, \ldots, m_k$ are pairwise relatively prime (so that the prime factors of m_i do not appear as prime factors of m_j for $j \neq i$), then any system of equation $x = a_i \pmod{m_i}$ for $i = 1, \ldots, k$ has exactly one solution defined modulo n, where $n = m_1 \cdots m_k$. In particular, $\varphi(n) = \varphi(m_1) \cdots \varphi(m_k)$.
Proof: For each $a \in \mathbb{Z}$, and each $i \in \{1, \ldots, k\}$, one associates the remainders a_i of the division of a by m_i, and then $a, b \in \mathbb{Z}$ have the same images if and only if $b - a$ is a multiple of m_i for all i, and this means that $b - a$ is a multiple of n. This shows that the mapping restricted to $\{0, \ldots, n-1\}$ is injective, but since the image belongs to the product $\{(a_1, \ldots, a_k) \mid 0 \leq a_i \leq m_i - 1, i = 1, \ldots, k\}$ which has n elements, it is also surjective.

An integer $a \in \mathbb{Z}$ is relatively prime with n if it has no common prime factors with n, which is that it has no common prime factors with any of the m_i, i.e. each a_i is relatively prime with m_i, and since there are $\varphi(m_i)$ such values of a_i, and there is an inverse mapping from the $a_i, i \in I$, to the solution x of the congruences in $\{0, \ldots, n-1\}$, the number of such a belonging to $\{0, \ldots, n-1\}$ is $\varphi(m_1) \cdots \varphi(m_k)$.

Definition 4.20: A mapping f from $\mathbb{N}^\times$ to $\mathbb{N}$ (or to $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$) is *multiplicative* if $f(a\,b) = f(a)\,f(b)$ whenever $(a, b) = 1$, and $f(1) = 1$.[18]

f is *completely multiplicative* if $f(a\,b) = f(a)\,f(b)$ for all a, b, and $f(1) = 1$.

Remark 4.21: The Euler function φ is multiplicative, and other multiplicative functions are used in number theory, but the basic observation is that given any list $a_{p,k}$ indexed on the primes p and the positive integers $k \geq 1$, there exists a unique multiplicative function f such that $f(p^k) = a_{p,k}$ for all primes p and all $k \geq 1$, since each n has a factorization $n = p_1^{k_1} \cdots p_r^{k_r}$, and one must have $f(n) = f(p_1^{k_1}) \cdots f(p_r^{k_r}) = a_{p_1,k_1} \cdots a_{p_r,k_r}$. Similarly, given any list a_p indexed on the primes, there exists a unique completely multiplicative function g such that $g(p) = a_p$ for all prime p, since one must have $g(n) = f(p_1)^{k_1} \cdots f(p_r)^{k_r} = a_{p_1}^{k_1} \cdots a_{p_r}^{k_r}$.

[17] So that e is replaced by 0, and $a^d = e$ is replaced by $d\,a = 0$. When working in $\mathbb{Z}_n$, one often switches from using equivalence classes or elements of $\mathbb{Z}$, so that $a = b$ is interpreted as $a = b \pmod{n}$ if $a, b \in \mathbb{Z}$.

[18] Often, $f(n)$ is only defined for $n \geq 2$ and satisfies $f(a\,b) = f(a)\,f(b)$ whenever $(a, b) = 1$ and $a, b \geq 2$, so that after defining $f(1) = 1$ it becomes true for $a, b \geq 1$. A basic example is to consider a polynomial $P \in \mathbb{Z}[x]$, i.e. having integer coefficients, and for $n \geq 2$ to define $f(n)$ as the number of solutions of $P(x) = 0$ modulo n, and the Chinese remainder theorem shows that for $a, b \geq 2$ and relatively prime one has $f(a\,b) = f(a)\,f(b)$.

Definition 4.22: A *primitive root modulo n* is any integer (when it exists) whose powers give (modulo n) all the integers relatively prime with n, i.e. it is a generator of the multiplicative group $\mathbb{Z}_n^*$ of units in $\mathbb{Z}_n$ (so that it cannot exist unless this group is cyclic).

Remark 4.23: Since for a prime p and $k \geq 1$ one has $\varphi(p^k) = p^k - p^{k-1}$ (because there are p^{k-1} multiples of p in $\{0, \ldots, p^k - 1\}$), one sees that besides $\varphi(2) = 1$, all other $\varphi(p^k)$ are even, so that Euler's theorem is not optimal if n has two distinct odd prime factors: for example, $\varphi(35) = \varphi(5)\,\varphi(7) = 4 \cdot 6 = 24$, but for a relatively prime with 35 one has $a^4 = 1 \pmod 5$ and $a^6 = 1 \pmod 7$, so that (12 being the lcm of 4 and 6) a^{12} is $= 1 \pmod 5$ and $= 1 \pmod 7$, hence $= 1 \pmod{35}$, and it means that in $\mathbb{Z}_{35}^*$ (which has 24 elements) all the orders of elements are divisors of 12, so that $\mathbb{Z}_{35}^*$ is not cyclic and there does not exist a primitive root modulo 35.

If a is odd one has $a^2 = 1 \pmod 8$, since $(2n+1)^2 = 4n\,(n+1)+1$ and $n\,(n+1)$ is even, so that Euler's theorem is not optimal for $n = 8$. By induction, using $(1 + b\,2^j)^2 = 1 + c\,2^{j+1}$ with $c = b + b^2 2^{j-1}$ for $j \geq 1$, one deduces that $a^{2^{k-2}} = 1 \pmod{2^k}$ for $k \geq 3$, and since $2^{k-2} = \frac{\varphi(2^k)}{2}$, Euler's theorem is not optimal for $n = 2^k$ and $k \geq 3$. One deduces that the only possible values n for which a primitive root modulo n may exist are $n = 2, 4, p^k$, or $2p^k$ for an odd prime p and $k \geq 1$. Since $\mathbb{Z}_2^* = \{1\}$ a primitive root modulo 2 is 1, and since $\mathbb{Z}_4^* = \{1, 3\}$ with $3 \cdot 3 = 1 \pmod 4$ a primitive root modulo 4 is 3.

It was shown by LEGENDRE,[19] and by GAUSS that for each odd prime p a primitive root modulo p exists, so that $\mathbb{Z}_p^*$ (with multiplication) is cyclic, i.e. isomorphic to $\mathbb{Z}_{p-1}$ (with addition) and since $\mathbb{Z}_{p-1}$ has $\varphi(p-1)$ generators, there are actually $\varphi(p-1)$ primitive roots modulo p; however, the proof of existence is a counting argument which is not an algorithm, so that it does not tell how to find such a primitive root. An important ingredient in the proof (which will be shown later in the course) is that a polynomial of degree d with coefficients in a field (here $\mathbb{Z}_p$) cannot have more than d roots.[20] Starting from a primitive root a modulo an odd prime p, it will be shown how to construct a primitive root b modulo $n = p^k$, and a primitive root c modulo $2p^k$, so that the values of n for which $\mathbb{Z}_n^*$ is cyclic are $n = 2, 4, p^k$, or $2p^k$ for an odd prime p and $k \geq 1$; there are $\varphi\big(\varphi(n)\big)$ primitive roots modulo n for such values of n, and for $n = p^k$ or $2p^k$ one has $\varphi(n) = p^{k-1}(p-1)$, so that there are $p^{k-2}(p-1)\,\varphi(p-1)$ primitive roots modulo n.

It will also be shown later that for any field F, if G is a finite subgroup of the multiplicative group F^*, then G is cyclic; the proof involves degrees of elements, and the fact that a polynomial of degree d with coefficients in F cannot have more than d roots.

Additional footnotes: ADLEMAN,[21] RIVEST,[22] Adi SHAMIR,[23] WEIZMANN.[24]

[19] Adrien-Marie LEGENDRE, French mathematician, 1752–1833. He worked in Paris, France.

[20] We have seen that $x^2 = 1$ has 4 roots in $\mathbb{Z}_8$, but this happens because $\mathbb{Z}_8$ is not an ID (integral domain), since $2 \cdot 4 = 0$ in $\mathbb{Z}_8$).

[21] Leonard Max ADLEMAN, American computer scientist and biologist, born in 1945. He works at USC (University of Southern California), Los Angeles, CA. The RSA public key cryptography algorithm, which he introduced in 1977 with RIVEST and Adi SHAMIR, is partially named after him.

[22] Ronald Linn RIVEST, American cryptologist, born in 1947. The RSA public key cryptography algorithm, which he introduced in 1977 with A. SHAMIR and ADLEMAN, is partially named after him.

[23] Adi SHAMIR, Israeli cryptologist, born in 1952. He works at the Weizmann Institute of Science, Rehovot, Israel. The RSA public key cryptography algorithm, which he introduced in 1977 with RIVEST and ADLEMAN, is partially named after him.

[24] Chaim WEIZMANN, Russian-born chemist, 1874–1952. He was the first president of Israel, 1949–1952. The Weizmann Institute of Science, Rehovot, Israel, is named after him.