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

36- Friday December 2, 2011.

Remark 36.1: The argument of EUCLID that there are infinitely many primes consists in assuming that there are only finitely many primes $p_1, \ldots, p_k$, and to consider $N = 1 + p_1 \cdots p_k$, which certainly has a prime factor (possibly itself) which is not in the list, since $N = 1 \pmod{p_j}$ for $j = 1, \ldots, k$.

There are simple variants for showing that in a particular arithmetic progression $a\,n + b$ with $a \geq 3$ and $(a, b) = 1$ there are infinitely many primes, but it is limited to $\varphi(a) \leq 2$, i.e. $a = 3, 4, 6$ for the value of $b \neq 1$; there is an improvement using quadratic residue theory, but it is limited to $\varphi(a) \leq 4$; then, using cyclotomic polynomials will give the case $b = 1$.

It is useful to know that DIRICHLET proved the result for all cases, that for $a \geq 3$ and b relatively prime with a, there are infinitely many values of n for which $a\,n+b$ is prime;[1] however, his proof belongs to *analytic* number theory, and not to *algebraic* number theory. Since there are $\varphi(a)$ families, it is natural to wonder in which of these families the primes fall, and each family has "asymptotic density" $\frac{1}{\varphi(a)}$ by a result of DE LA VALLÉE POUSSIN,[2] who improved a previous result of DIRICHLET for another notion of density, related to Dirichlet series.

Lemma 36.2: There are infinitely many primes of the form $6n - 1$ (hence infinitely many primes of the form $3n - 1$), and there are infinitely many primes of the form $4n - 1$. More generally, for each $a \geq 3$ there are infinitely many primes of the form $a\,n + b$ for *some* $b \neq 1$, i.e. which are *not* of the form $a\,n + 1$.
Proof: If there was only finitely many primes $q_1 < \ldots < q_k$ not of the form $a\,n + 1$, then $N = a\,q_1 \cdots q_k - 1$ would be of the form $a\,n - 1$, so that the prime factors of N could not prime divisors of a, but they could not be all of the form $a\,n+1$ since the product would also have this form (and $-1 \neq 1 \pmod{a}$ since $a = 2$ is excluded), so that N would have a prime divisor not of the form $a\,n+1$, but it could not be any q_j, giving a contradiction.

If $\varphi(a) = 2$, i.e. $a \in \{3, 4, 6\}$, then it tells the form of the family in which these primes fall, i.e. $3n - 1$, $4n - 1$, $6n - 1$.

Lemma 36.3: There are infinitely many primes of the form $4n + 1$.
Proof: One has seen that -1 is a quadratic residue modulo an odd prime p if and only if p is of the form $4m + 1$, and one deduces that (whatever N is) all the (necessarily odd) prime divisors of $4N^2 + 1$ are of the form $4m+1$, since if p is such a prime divisor one has $(2N)^2 = -1 \pmod{p}$, hence -1 is a quadratic residue modulo p. If the only primes of the form $4n + 1$ were $5 = p_1, \ldots, p_k$, then one would take $N = p_1 \cdots p_k$, and obtain a contradiction.

Remark 36.4: If a prime p has the form $4n + 1$, one can deduce that -1 is a quadratic residue by using a primitive root ξ modulo p: ξ has order $4n$ in $\mathbb{Z}_p^*$, so that $(\xi^{2n})^2 = 1$ and $\xi^{2n} \neq 1$ imply $\xi^{2n} = -1$, hence the solutions of $a^2 = -1 \pmod{p}$ are $a = \pm\xi^n \pmod{p}$.

Similarly, if a prime q is $4n+3$, one can deduce that -1 is not a quadratic residue modulo q: one chooses a primitive root η modulo q, and if -1 was the square of b, b would be η^j for some j, so that $-1 = \eta^{2j}$, hence $1 = \eta^{4j}$, which implies that $4j$ would a multiple of $q - 1$ but $2j$ would not be a multiple of $q - 1$, and this is contradictory, since $4j = k\,(q - 1)$ implies k even (because $2j = k\,(2n + 1)$), so that $k = 2\ell$, hence $2j = \ell\,(q - 1)$.

Lemma 36.5: (Gauss's lemma)[3] Let $p = 2m + 1$ be an odd prime. For a not a multiple of p, and for $j \in \{1, \ldots, m\}$ one writes $j\,a = \alpha_j \pmod{p}$ with $\alpha_j \in \{1, \ldots, 2m\}$, and one defines $g(a)$ as the number of α_j which belong to $\{m + 1, \ldots, 2m\}$. Then, one has $\left(\frac{a}{p}\right) = (-1)^{g(a)}$.

[1] Of course, in an arithmetic progression $a\,n + b$ where n varies, all the terms are multiple of $d = (a, b)$, so that if a and b are not relatively prime one finds at most one prime in the arithmetic progression, if d is prime.

[2] Charles Jean Gustave Nicolas DE LA VALLÉE POUSSIN, Belgian mathematician, 1866–1962. He was made baron in 1928. He worked in Louvain, Belgium.

[3] This is a different lemma of GAUSS than the one on irreducibility in $\mathbb{Z}[x]$.

Proof: Since a is invertible modulo p, the elements $j\,a$ are distinct modulo p, so that the α_j are distinct. For $j = 1,\ldots,m$, one defines β_j as $\min\{\alpha_j, p-\alpha_j\}$ (so that $1 \le \beta_j \le m$), and the number of indices j such that $\beta_j = p - \alpha_j$ is $g(a)$, hence $\prod_j \beta_j = (-1)^{g(a)} \prod_j \alpha_j = (-1)^{g(a)} \prod_j (j\,a) = (-1)^{g(a)} a^m m! \pmod p$. The elements $\{\beta_j \mid j = 1,\ldots,m\}$ are distinct, since one cannot have $\alpha_j = p - \alpha_k$, because one has $2 \le \alpha_j + \alpha_k \le 2m = p-1$ for all $j,k \in \{1,\ldots,m\}$, so that $\{\beta_1,\ldots,\beta_m\}$ is a permutation of $\{1,\ldots,m\}$, and $\prod_j \beta_j = m!$, hence $(-1)^{g(a)} a^m m! = m! \pmod p$. Since $m!$ is invertible modulo p, one deduces that $a^m = (-1)^{g(a)} \pmod p$, giving $\left(\frac{a}{p}\right) = (-1)^{g(a)}$.

Lemma 36.6: For p an odd prime, one has $\left(\frac{2}{p}\right) = +1$ if and only if p has the form $8n \pm 1$, and $\left(\frac{2}{p}\right) = -1$ if and only if p has the form $8n \pm 3$, which analytically means that $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.

As a consequence, one has $\left(\frac{-2}{p}\right) = +1$ if and only if p has the form $8n+1$ or $8n+3$, and $\left(\frac{-2}{p}\right) = -1$ if and only if p has the form $8n+5$ or $8n+7$.

Proof: One applies Gauss's lemma (Lemma 36.5) to $a = 2$, so that if $p = 2m+1$ one has $\alpha_j = 2j$ for $j = 1,\ldots,m$, and $\alpha_j \ge m+1$ means $j \ge \frac{m+1}{2}$: if $m = 2r$, it means $j \ge r+1$, so that $g(a) = r$ and $g(a)$ is even if and only if p has the form $8n+1$, while if $m = 2r+1$, it also means $j \ge r+1$, but $g(a) = r+1$, so that $g(a)$ is even if r is odd, i.e. m has the form $4n+3$ and p has the form $8n+7$ (which is the same as the form $8n-1$).

Then, one uses $\left(\frac{-2}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{-1}{p}\right)$, together with the fact that -1 is a quadratic residue modulo p if and only if p has the form $4n+1$.

Lemma 36.7: There are infinitely many primes of the form $8n+7$, and there are infinitely many primes of the form $8n+3$.[4]

Proof: If there were only a finite number of primes $7 = p_1 < \ldots < p_k$ of the form $8n+7$, then for $N = p_1 \cdots p_k$ any prime factor s of $8N^2-1$ would be either of the form $8n+1$ or of the form $8n+7$ by Lemma 36.6, since 2 is a quadratic residue modulo s, because $2(8N^2-1) = 0 \pmod s$ means $2 = (4N)^2 \pmod s$; since $8N^2-1$ is odd and its prime factors cannot all be of the form $8n+1$, because their product would have this form, there would be at least one prime factor s of the form $8n+7$, which could not belong to the list $\{p_1,\ldots,p_k\}$, made of divisors of N.

If there were only a finite number of primes $3 = q_1 < \ldots < q_k$ of the form $8n+3$, then for $M = q_1 \cdots q_k$ any prime factor t of $2M^2+1$ would be either of the form $8n+1$ or of the form $8n+3$ by Lemma 36.6, since -2 is a quadratic residue modulo t, because $2(M^2+1) = 0 \pmod t$ means $(2M)^2 = -2 \pmod t$; since $2M^2+1$ is odd and its prime factors cannot all be of the form $8n+1$, because their product would have this form (and M being odd implies $2M^2+1 = 3 \pmod 8$), there would be at least one prime factor t of the form $8n+3$, which could not belong to the list $\{q_1,\ldots,q_k\}$, made of divisors of M.

Remark 36.8: One may expect the preceding idea to work for proving that there are infinitely many primes in some family of the form $a\,n+b$ if $\varphi(a) = 4$, by finding a quadratic residue which only occurs for the form $a\,n+1$ or $a\,n+\beta$ for a particular value of β (and not for the other two families). One has $\varphi(a) = 4$ for $a \in \{5,8,12\}$, and the argument does work for $a = 5$ and for $a = 12$, but it uses the law of quadratic reciprocity, which is then a more technical step: recall that it was conjectured by LEGENDRE, who could not prove it, and EULER could not prove it either, but GAUSS published six different proofs.

Lemma 36.9: If $P \in \mathbb{Z}[x]$ is a (non-constant) monic polynomial, then there are infinitely many prime divisors of the sequence $P(1), P(2)\ldots, P(n), \ldots$.

Proof: Suppose that $p_1,\ldots,p_k$ are the only prime divisors of the sequence, and let $N = p_1 \cdots p_k$. Since P has at most $deg(P)$ zeros, there exists $m \ge 1$ such that $P(m) = a \ne 0$, and then the Taylor expansion of $P(m + a\,N\,x)$ at m has all its coefficients multiple of a, since it is $\sum_j c_j x^j$ with $c_0 = P(m) = a \in \mathbb{Z}$, and $c_j = \frac{P^{(j)}(m)}{j!} a^j N^j$ for $j \ge 1$, which is a multiple of a since $\frac{P^{(j)}(m)}{j!} \in \mathbb{Z}$.[5] One deduces that $Q(x) = \frac{P(m+a\,N\,x)}{a} \in \mathbb{Z}[x]$, but also that $Q(n) = 1 + \sum_{j\ge 1} \frac{P^{(j)}(m)}{j!} a^{j-1} N^j n^j = 1 \pmod N$ for all $n \ge 1$, and

[4] This is more precise than the part of Lemma 36.2 which says that there are infinitely many primes of the form $4n+3$.

[5] For $P = \sum_{i\ge 0} \alpha_i x^i \in \mathbb{Z}[x]$, one has $\frac{P^{(j)}}{j!} = \sum_{i \ge j} \alpha_i \binom{i}{j} x^{i-j} \in \mathbb{Z}[x]$.

since there are only a finite number of n for which $Q(n) = 1$, there exists n with $Q(n) > 1$ and $Q(n) = 1 \pmod{N}$, so that $Q(n)$ must have a prime factor not in the list $\{p_1, \ldots, p_k\}$, hence $P(m + a\,N\,n) = a\,Q(n)$ has a prime factor not in the list $\{p_1, \ldots, p_k\}$.

Lemma 36.10: For $m \geq 3$, let p be an odd prime not dividing m, and such that the cyclotomic polynomial Φ_m satisfies $\Phi_m(a) = 0 \pmod{p}$ for some $a \in \mathbb{Z}$. Then, a is not a multiple of p, and the order of a in $\mathbb{Z}_p^*$ is exactly m, so that m divides $p-1$, i.e. $p = 1 \pmod{m}$.
Proof: Since $x^m - 1 = \Phi_m \prod_{d|m, d\neq m} \Phi_d$, $a^m - 1$ is a multiple of $\Phi_m(a)$, so that $a^m - 1 = 0 \pmod{p}$, hence a is not a multiple of p. If the order of a in $\mathbb{Z}_p^*$ was $d < m$, d would be a divisor of m, and from $a^d = 1 \pmod{p}$ one would deduce that $\Phi_\delta(a) = 0 \pmod{p}$ for a divisor δ of d, hence a divisor of m (different from m), so that $x^m - 1$ would have a as a (non-zero) repeated root in $\mathbb{Z}_p$ (since Φ_m and Φ_δ would be divisible by $(x-a)$), contradicting the fact that $m\,x^{m-1}$, the derivative of $x^m - 1$, is $\neq 0$ on $\mathbb{Z}_p^*$ (because p is not a divisor of m). The order of a is then m, and since $a^{p-1} = 1 \pmod{p}$ by Fermat's theorem, one deduces that $p-1$ is a multiple of m.

Lemma 36.11: For any integer $m \geq 3$, there are infinitely many primes equal to 1 modulo m.
Proof: By Lemma 36.10, if p is a prime factor of $\Phi_m(a)$, then either p divides m or $p = 1 \pmod{m}$, but by Lemma 36.9 there are infinitely many prime divisors of $\Phi_m(1), \Phi_m(2), \ldots$, and one deduces that infinitely many of these primes are equal to 1 modulo m, since there are only a finite number of prime divisors of m.