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

6- Monday September 12, 2011.

Remark 6.1: If $P \in \mathbb{Z}[x]$, i.e. if P is a polynomial with integer coefficients, then $P(a) \in \mathbb{Z}$ for all $a \in \mathbb{Z}$, and it is easy to see that if P has an integer root a, i.e. $P(a) = 0$, then a divides the constant coefficient, which is $P(0)$, but such an argument does not work if one looks for solutions modulo n for some $n \geq 2$. If for $n \geq 2$, one defines $f(n)$ as the number of solutions in $\mathbb{Z}_n$ of the equation $P(a) = 0 \pmod{n}$, then the Chinese remainder theorem shows that $f(m\,n) = f(m)\,f(n)$ whenever m and n are relatively prime (and ≥ 2), so that by defining $f(1) = 1$ one deduces that f is a multiplicative function.

Remark 6.2: Before the Euler function φ, other particular multiplicative functions had been introduced in number theory, like $\sigma_k(n) = \sum_{d|n} d^k$, so that $\sigma_0(n)$ is the number of divisors of n, and $\sigma_1(n)$ is the sum of divisors of n (including n), which appears in the definition of a *perfect number* n, which is equal to the sum of its proper divisors, i.e. such that $\sigma_1(n) = 2n$. It was noticed early that 6 and 28 are perfect, and EUCLID observed that if $p = 2^m - 1$ is prime, then $2^{m-1}(2^m - 1)$ is a perfect number,[1] but such primes are now called *Mersenne primes*.[2] The next two perfect numbers are 496 $(16 \cdot 31)$ and 8 128 $(64 \cdot 127)$, noticed by NICOMACHUS,[3] and the next is 33 550 336, which was recorded in 1456 by an unknown mathematician, and then CATALDI found the next two (8 589 869 056 and 137 438 691 328) in 1588.[4]

It is not known if there are infinitely many Mersenne primes, and the first 40 correspond to m equal to 2, 3, 5, 7, 13, 17, 19,[5] 31,[6] 61, 89, 107, 127, 521, 607, 1 279, 2 203, 2 281, 3 217, 4 253, 4 423, 9 689, 9 941, 11 213, 19 937, 21 701, 23 209, 44 497, 86 243, 110 503, 132 049, 216 091, 756 839, 859 433, 1 257 787, 1 398 269, 2 976 221, 3 021 377, 6 972 593, 13 466 917, 20 996 011, and it is not clear what the next value of m is, but 7 more are known (24 036 583, 25 964 951, 30 402 457, 32 582 657, 37 156 667, 42 643 801, 43 112 609). ALHAZEN (Ibn al-Haytham) conjectured that every even perfect number has the form used by EUCLID,[7] and this was proved by EULER.[8]

It is not known if there exist odd perfect numbers.

Definition 6.2: For two mappings f, g from $\mathbb{N}^\times$ into $\mathbb{Z}$ (or $\mathbb{Q}$, $\mathbb{R}$, or $\mathbb{C}$) one defines $h = f \star g$ by $h(n) = \sum_{d|n} f(d)\,g\big(\frac{n}{d}\big)$.

---

[1] Since $\sigma_1(2^{m-1}) = 1 + 2 + \ldots + 2^{m-1} = 2^m - 1$, and for p prime $\sigma_1(p) = p + 1$, then $2^{m-1}p$ perfect means $(2^m - 1)\,(p + 1) = 2^m p$, i.e. $p = 2^m - 1$.

[2] Marin MERSENNE, French mathematician, 1588–1648. Mersenne primes numbers (of the form $2^k - 1$) are named after him.

[3] NICOMACHUS of Gerasa (now Jarash, Jordan), Greek mathematician, 60–120.

[4] Pietro Antonio CATALDI, Italian mathematician, 1548–1626. He worked in Perugia and in Bologna, Italy.

[5] CATALDI proved that $2^{19} - 1$ is prime by dividing it by all the primes up to its square root, so that he first computed all the primes up to 750.

[6] EULER first showed that all prime divisors of $2^{31} - 1$ must have the form $248n + 1$ or $248n + 63$, and then he divided $2^{31} - 1$ by all such primes less than 46 339: since 31 is prime it is the order of 2 in $\mathbb{Z}_p^*$, so that 31 divides $p - 1$, and since $p - 1$ is even, one has $p = 62r + 1$ for some r; since $2^{32} = 2 \pmod{p}$, 2 is a quadratic residue modulo p, which means that $p = \pm 1 \pmod{8}$, and $p = 8s + 1$ implies $r = 4n$, while $p = 8s - 1$ implies $r = 4n + 1$, hence the forms $248n + 1$ or $248n + 63$ for p. EULER had used the same argument for showing that $F_5 = 2^{32} + 1$ is not prime: if p is an odd prime divisor of F_5, 2 has order 64 in $\mathbb{Z}_p^*$ (since the order divides 64 but does not divide 32), so that $p = 64a + 1$, and then by restricting the trials to such primes he found that 641 is a divisor of F_5; actually, since 2 is a quadratic residue modulo p (because $p = 1 \pmod{8}$), one has $2 = b^2 \pmod{p}$, then b has order 128 in $\mathbb{Z}_p^*$, so that p has the form $128c + 1$.

[7] ALHAZEN (Abu 'Ali al-Hasan ibn al-Hasan ibn al-Haytham), Persian mathematician, 965–1040.

[8] If $2^k M$ is perfect with $k \geq 1$ and M odd, then $\sigma_1(2^k M) = (2^{k+1} - 1)\,\sigma_1(M) = 2^{k+1} M$, so that $2^{k+1} - 1$ divides M, so that $M = (2^{k+1} - 1)\,r$ and $\sigma_1(M) = 2^{k+1} r$; $r = 1$ gives $\sigma_1(M) = 2^{k+1} = M + 1$, hence M must be prime; $r > 1$ implies $\sigma_1(M) \geq 1 + r + M$, which is $1 + 2^{k+1}\,r$, a contradiction.

Remark 6.3: That $\star$ is commutative is seen by replacing d by $\frac{n}{d}$, or by writing in a symmetric way $h(n) = \sum_{d_1 d_2 = n} f(d_1)\, g(d_2)$. Then $(f \star g) \star k = \ell$ means $\ell(n) = \sum_{d_1 d_2 d_3 = n} f(d_1)\, g(d_2)\, k(d_3)$, which is also the formula for $f \star (g \star k)$, so that $\star$ is associative. There is an identity element δ defined by $\delta(1) = 1$ and $\delta(n) = 0$ for $n \geq 2$.

In analysis, $\star$ is the symbol for convolution, which here is related to using the multiplicative group $\mathbb{R}_+$ and its Haar measure $\frac{dt}{t}$:[9] for continuous functions with compact support in $(0, \infty)$, $h = f \star g$ means $h(x) = \int_0^\infty f(s)\, g\big(\frac{t}{s}\big)\, \frac{ds}{s}$, but in order to deduce Definition 6.2, one must let the continuous functions approach combination of Dirac masses at the integer points.[10]

Lemma 6.4: If f and g are multiplicative functions, then $f \star g$ is multiplicative, and the set of multiplicative functions with $\star$ (and δ as identity) is a group.
Proof: For a_1 and a_2 relatively prime (so that they have different prime factors), and d a divisor of $a_1 a_2$, one has a unique decomposition as $d = d_1 d_2$ where d_1 is a divisor of a_1 and d_2 is a divisor of a_2. Then $h(a_1 a_2) = \sum_{d | a_1 a_2} f(d)\, g\big(\frac{a_1 a_2}{d}\big) = \sum_{d_1 | a_1, d_2 | a_2} f(d_1 d_2)\, g\big(\frac{a_1 a_2}{d_1 d_2}\big)$, but since $f(d_1 d_2) = f(d_1)\, f(d_2)$ and $g\big(\frac{a_1 a_2}{d_1 d_2}\big) = g\big(\frac{a_1}{d_1}\big)\, g\big(\frac{a_2}{d_2}\big)$, one has $h(a_1 a_2) = \sum_{d_1 | a_1, d_2 | a_2} f(d_1)\, f(d_2)\, g\big(\frac{a_1}{d_1}\big)\, g\big(\frac{a_2}{d_2}\big)$, which is $\sum_{d_1 | a_1} f(d_1)\, g\big(\frac{a_1}{d_1}\big)$ times $\sum_{d_2 | a_2} f(d_2)\, g\big(\frac{a_2}{d_2}\big)$ i.e. $h(a_1)\, h(a_2)$.

For constructing the inverse of f, one looks for a multiplicative function ψ such that $f \star \psi(p^k) = \delta(p^k)$ for all primes p and all $k \geq 1$, and one checks that it characterizes all the values of $\psi(p^k)$, and there is a unique extension to all values $n \in \mathbb{N}^\times$, and the product $f \star \psi$ is then a multiplicative function taking the same values than δ on the powers of primes, so that it is δ. For doing this, one first takes $\psi(1) = 1$, so that $f \star \psi(1) = 1 = \delta(1)$; then $f \star \psi(p) = \delta(p) = 0$ gives $\psi(p) + f(p) = 0$, so that $\psi(p)$ is defined (and belongs to $\mathbb{Z}$ if f takes its values in $\mathbb{Z}$); $f \star \psi(p^2) = \delta(p^2) = 0$ gives $\psi(p^2) + f(p)\, \psi(p) + f(p^2) = 0$, so that $\psi(p^2)$ is defined (and belongs to $\mathbb{Z}$ if f takes its values in $\mathbb{Z}$), and by induction one deduces that all the values $\psi(p^k)$ are characterized.

Definition 6.5: The multiplicative function μ defined by $\mu(1) = 1$ and, for each prime p, $\mu(p) = -1$ and $\mu(p^k) = 0$ for $k \geq 2$ is the *Möbius function*.[11]

Remark 6.6: Apart from $n = 1$, one has $\mu(n) \neq 0$ only if n is square-free, i.e. $n = p_1 \cdots p_k$ for distinct primes, in which case $\mu(n) = (-1)^k$.

Lemma 6.7 (Möbius's inversion formula) If for any function f one defines F by $F(n) = \sum_{d | n} f(d)$ for all n, then one has $f(n) = \sum_{d | n} \mu(d)\, F\big(\frac{n}{d}\big)$.
Proof: If one defines $\mathbf{1}$ by $\mathbf{1}(n) = 1$ for all n, so that $\mathbf{1}$ is completely multiplicative, then one checks that $\mu \star \mathbf{1}(1) = 1$ and $\mu \star \mathbf{1}(p^k) = 0$ for all primes p and all $k \geq 1$, so that $\mu \star \mathbf{1} = \delta$. Then the formula defining F is precisely $F = \mathbf{1} \star f$, so that $\mu \star F = \mu \star (\mathbf{1} \star f) = (\mu \star \mathbf{1}) \star f = \delta \star f = f$, which is Möbius's inversion formula.

Remark 6.8: The "Riemann" *zeta function*, defined by $\zeta(s) = \sum_{n=1}^\infty \frac{1}{n^s}$ was introduced by EULER in his thesis, and he observed that it factorizes as $\prod_p \frac{1}{1 - \frac{1}{p^s}}$, where the product is indexed by primes, but EULER lived much before CAUCHY had properly defined the notions of convergence of series of functions, and the definition of holomorphic or meromorphic functions of a complex variable z, so that such questions concerning the zeta function were not done by EULER but by RIEMANN; besides the obvious fact that the series converges uniformly if $\Re(s) > 1$, he showed that the zeta function can be extended analytically to the whole complex plane except for a simple pole at $s = 1$ (where $\zeta(s)$ behave as $\frac{1}{s-1}$), and that this meromorphic

[9] Alfréd HAAR, Hungarian mathematician, 1885–1933. He worked at Georg-August-Universität, Göttingen, Germany, in Kolozsvár (then in Hungary, now Cluj-Napoca, Romania), in Budapest and in Szeged, Hungary.

[10] Paul Adrien Maurice DIRAC, English physicist, 1902–1984. He received the Nobel Prize in Physics in 1933, jointly with Erwin SCHRÖDINGER, for the discovery of new productive forms of atomic theory. He worked in Cambridge, England, holding the Lucasian chair (1932–1969).

[11] August Ferdinand MÖBIUS, German mathematician, 1790–1868. He worked in Leipzig, Germany. The Möbius function and the Möbius inversion formula are named after him. The "Möbius" strip is also named after MÖBIUS, but it was introduced before him by LISTING.

function satisfies a functional equation $\zeta(s) = 2^s \pi^{s-1} \sin\left(\frac{\pi\, s}{2}\right) \Gamma(1-s)\, \zeta(1-s)$, or more symmetrically $\Gamma\left(\frac{s}{2}\right) \pi^{-s/2} \zeta(s) = \Gamma\left(\frac{1-s}{2}\right) \pi^{-(1-s)/2} \zeta(1-s)$, where the *Gamma function* is given by $\Gamma(z) = \int_0^{+\infty} t^{-z} e^{-t}\, dt$ (introduced by EULER) and satisfies $\Gamma(z+1) = z\, \Gamma(z)$ and $\Gamma(n) = (n-1)!$ for all $n \in \mathbb{N}^\times$. Besides "trivial zeros" at $-2, -4, \ldots$, the zeros of the zeta function lie in the *critical strip* $0 < \Re(s) < 1$ and the *Riemann hypothesis* is a conjecture by RIEMANN that they all lie on the line $\Re(s) = \frac{1}{2}$: there is a one million dollar Clay Prize for proving (or disproving) this conjecture.[12]

Remark 6.9: DIRICHLET generalized such remarks by associating to a function f its *Dirichlet series* $F(s) = \sum_{n=1}^{\infty} \frac{f(n)}{n^s}$;[13] if f satisfies a growth estimate $|f(n)| \leq A\, n^\alpha$ for all $n \in \mathbb{N}^\times$ with $\alpha \geq 0$, then $F(s)$ is well defined for $\Re(s) > \alpha + 1$ with a bound $|F(s)| \leq A\, \frac{\Re(s)-\alpha}{\Re(s)-\alpha-1}$.[14]

If g satisfies a growth estimate $|g(n)| \leq B\, n^\alpha$ for all $n \in \mathbb{N}^\times$ with $\alpha \geq 0$, then the Dirichlet series $G(s)$ is well defined for $\Re(s) > \alpha + 1$ with a bound $|G(s)| \leq B\, \frac{\Re(s)-\alpha}{\Re(s)-\alpha-1}$, and if $h = f \star g$, then it satisfies the growth estimate $|h(n)| \leq A\, B\, n^\alpha \sigma_0(n)$ for all $n \in \mathbb{N}^\times$,[15] and its Dirichlet series is $H(s) = F(s)\, G(s)$ in the region $\Re(s) > \alpha + 1$,[16] with the bound $|H(s)| \leq A\, B\, \frac{(\Re(s)-\alpha)^2}{(\Re(s)-\alpha-1)^2}$.

If f is multiplicative and satisfies $|f(n)| \leq n^\alpha$ for all $n \in \mathbb{N}^\times$ with $\alpha \geq 0$, then for $\Re(s) > \alpha + 1$ the Dirichlet series $F(s)$ can be written as an *Euler product* $\prod_p F_p(s)$ over the primes, where $F_p(s) = \sum_{k \geq 0} \frac{f(p^k)}{p^{k\, s}}$, so that $|F_p(s)| \leq \frac{1}{1-p^{\alpha-s}}$ and the product is uniformly convergent.

In particular, the Dirichlet series $M(s) = \sum_{n \geq 1} \frac{\mu(n)}{n^s}$ (uniformly convergent in $\Re(s) > 1$) associated to the Möbius function is $\frac{1}{\zeta(s)}$, so that the Riemann hypothesis is equivalent to the conjecture that $M(s)$ extends to an holomorphic function in $\Re(s) > \frac{1}{2}$.

The Dirichlet series $\Phi(s) = \sum_{n \geq 1} \frac{\varphi(n)}{n^s}$ (uniformly convergent in $\Re(s) > 2$) associated to the Euler function is $\frac{\zeta(s-1)}{\zeta(s)}$.

Additional footnotes: GREEN,[17] LISTING,[18] LUCAS H.,[19] PERSE,[20] SCHRÖDINGER.[21]

---

[12] Landon Thomas CLAY, American investment banker and philanthropist, born in 1926.

[13] Johann Peter Gustav LEJEUNE DIRICHLET, German mathematician, 1805–1859. He worked in Breslau (then in Germany, now Wrocław, Poland), in Berlin, and at Georg-August-Universität, Göttingen, Germany. Dirichlet series, and the Dirichlet conditions are named after him. The Dirichlet principle was named after DIRICHLET by RIEMANN, who was probably unaware that GAUSS and GREEN had used the same idea before him.

[14] By comparing a series with an integral: if ψ is a positive non-increasing function, then $\int_1^\infty \psi(x)\, dx \leq \sum_{n=1}^\infty \psi(n) \leq \psi(1) + \int_1^\infty \psi(x)\, dx$.

[15] Since each term $f(d) g\left(\frac{n}{d}\right)$ is bounded in absolute value by $A\, d^\alpha B\, \frac{n^\alpha}{d^\alpha} = A\, B\, n^\alpha$, and there are $\sigma_0(n)$ divisors d of n.

[16] For $\Re(s) > \alpha + 1$ one can make the product of the two series giving $F(s)$ and $G(s)$ and sum it in any way one likes, so that by pairing the terms in $f(d_1) g(d_2)$ corresponding to a value $d_1 d_2 = n$, the Dirichlet series for h appears.

[17] George GREEN, English mathematician, 1793–1841. He was a miller, and he wrote interesting articles before starting studying at Cambridge, at age 40; he received a Perse fellowship at Cambridge, England, but he did not live long afterward.

[18] Johann Benedict LISTING, German mathematician, 1808–1882. He worked at Georg-August-Universität, Göttingen, Germany. He introduced the "Möbius" strip before MÖBIUS.

[19] Reverend Henry LUCAS, English clergyman and philanthropist, 1610–1663. The Lucasian chair in Cambridge, England, is named after him.

[20] Stephen PERSE, English philanthropist, 1548–1615.

[21] Erwin Rudolf Josef Alexander SCHRÖDINGER, Austrian-born physicist, 1887–1961. He received the Nobel Prize in Physics in 1933, jointly with Paul Adrien Maurice DIRAC, for the discovery of new productive forms of atomic theory. He worked in Vienna, Austria, in Jena and in Stuttgart, Germany, in Breslau (then in Germany, now Wrocław, Poland), in Zürich, Switzerland, in Berlin, Germany, in Oxford, England, in Graz, Austria, and in Dublin, Ireland.