Comptes rendus mathématiques
Mathematical Reports

SEPTEMBRE / SEPTEMBER 1998

20
No 3

IN THIS ISSUE / DANS CE NUMÉRO

C. R. Math. Rep. Acad. Sci. Canada Vol. **20** (3), 1998 pp. 65–70

LIMITING BEHAVIOUR OF SOME COMBINATORIAL STRUCTURES IN POPULATION GENETICS

SHUI FENG AND FRED M. HOPPE

Presented by D. A. Dawson, FRSC

ABSTRACT. Large deviation principles are established for some combinatorial structures in population genetics including the Ewens sampling formula and its two-parameter generalization.

RÉSUMÉ. On établit des principes de grandes déviations pour certaines structures combinatoires en génétique de population, en particulier pour la formule d'échantillonnage de Ewens et sa généralisation á deux paramétres.

1. Introduction. A partition π of a positive integer n is an unordered representation of n as a sum of positive integers $n = n_1 + n_2 + \cdots + n_k$. It is customary to describe π as a multiplicity vector or "allelic partition" (*cf.* [9]) $m = (m_1, \ldots, m_n)$, where $m_j = m_j(\pi) = \sharp\{i : n_i = j\}$ is the number of times integer j appears in $\{n_1, \ldots, n_k\}$.

A random partition of n is a random variable Π_n with values in the finite set of all partitions of n. As an illustration, one of the random partitions Π_n^θ considered in this paper is the Ewens sampling formula introduced in [4]

$$P_n^\theta(m_1, m_2, \ldots, m_n) = P\big[\Pi_n^\theta = (m_1, \ldots, m_n)\big] = \frac{n!}{[\theta]^n} \Pi_{i=1}^n \frac{\theta^{m_i}}{i^{m_i}(m_i!)}. \tag{1.1}$$

Here $\theta > 0$ is a parameter and $[\theta]^n = \theta(\theta+1)\cdots(\theta+n-1)$ is the ascending factorial, and (1.1) describes the partition when a sample of size n is taken from a selectively neutral haploid population which has evolved towards equilibrium. This remarkable distribution also arises in many non-genetics contexts such as in Bayesian statistics [1], random permutations [13] and in a Pólya-like urn model [7].

Pitman [10], [11] described a two-parameter sampling formula with parameters $0 \le \alpha < 1$, $\theta > -\alpha$, denoted by $\Pi_n^{\alpha,\theta}$ and defined by

$$\begin{aligned} P_n^{\alpha,\theta}(m_1, m_2, \ldots, m_n) &= P\big[\Pi_n^{\alpha,\theta} = (m_1, m_2, \ldots, m_n)\big] \\ &= \frac{n!}{[\theta]^n} \Pi_{l=0}^{k-1}(\theta + l\alpha) \Pi_{i=1}^n \frac{\big([1-\alpha]^{i-1}\big)^{m_i}}{(i!)^{m_i}(m_i!)}. \end{aligned} \tag{1.2}$$

Received by the editors November 3, 1997.
Research supported by the Natural Sciences and Engineering Council of Canada.
AMS subject classification: Primary: 60F10; secondary: 05A17, 92D10.

The random partition $\Pi_n^{\alpha,\theta}$ arose in the study of stable processes with index α and in particular the case $\alpha = \frac{1}{2}$ is related to the zeros of Brownian motion and Brownian bridge. When $\alpha = 0$, $\Pi_n^{0,\theta} = \Pi_n^{\theta}$, the Ewens case.

In genetics the number of parts K_n^{θ} of Π_n^{θ} is the number of alleles in a sample of size n while in the context of random permutations K_n^{θ} represents the number of cycles in the cycle representation of a permutation chosen uniformly from all $n!$ permutations (in which case $\theta = 1$).

There have been many studies on the behaviour of K_n^{θ} as n goes to infinity. It is well-known that the following law of large numbers holds

$$\lim_{n\to\infty} \frac{K_n^{\theta}}{\log n} = \theta, \ a.s., \tag{1.3}$$

and Goncharov [5] obtained the following central limit theorem

$$\frac{K_n^{\theta} - \log n}{\sqrt{\log n}} \xrightarrow{\mathcal{D}} N(0,1). \tag{1.4}$$

If we write $K_n^{\theta}(t) = \sum_{i=1}^{[n^t]} m_i(t)$ and let

$$Y_n^{\theta}(t) = \frac{K_n^{\theta}(t) - \theta t \log n}{\sqrt{\theta \log n}}, \quad 0 \le t \le 1,$$

then Hansen [6] proved that $Y_n^{\theta}(\cdot)$ converges weakly to Wiener measure on the Skorohod space $D[0,1]$, which is a functional central limit theorem for the process $K_n^{\theta}(\cdot)$. Previously, DeLaurentis and Pittel [2] obtained this result for $\theta = 1$.

Next, let $K_n^{\alpha,\theta}$ denote the number of parts of $\Pi_n^{\alpha,\theta}$. Then for $\alpha > 0$ and general θ, (see [10], [12])

$$\lim_{n\to\infty} \frac{K_n^{\alpha,\theta}}{n^{\alpha}} = S_{\alpha,\theta}, \ a.s. \tag{1.5}$$

where $S_{\alpha,\theta}$ is related to the Mittag-Leffler distribution.

The main results of this paper are a path level large deviation principle for $K_n^{\theta}(t)$ and a large deviation principle for $K_n^{\alpha,\theta}$ as n goes to infinity. We now state the results and outline the proofs later.

THEOREM 1.1. *Let* $\mathbf{D}[0,1]$ *be the space* $D[0,T]$ *equipped with the uniform convergence topolology and let* ν_n^{θ} *be the law of* $K_n^{\theta}(t)/\log n$ *under* P_n^{θ} *in* (1.1). *Define*

$$S_{\theta}(f) = \int_0^1 I(\dot{f}(t))\, dt$$

$$= \begin{cases} \int_0^1 \dot{f}(t) \log\left(\frac{\dot{f}(t)}{\theta}\right) dt + \theta - f(1), & \text{if } f(0) = 0, \\ & \text{and } f \text{ is absolutely continuous} \\ \infty, & \text{otherwise.} \end{cases}$$

Then the sequence $\{\nu_n^\theta\}_{n\geq 1}$ *satisfies a large deviation principle on space* $\mathbf{D}[0,1]$ *with rate function* $S_\theta(\cdot)$ *and speed* $\log n$, *i.e., for any Borel set* $A \subset \mathbf{D}[0,1]$,

$$-\inf_{f\in A^\circ} S_\theta(f) \leq \liminf_{n\to\infty} \frac{1}{\log n}\nu_n^\theta(A) \leq \limsup_{n\to\infty} \frac{1}{\log n}\nu_n^\theta(A) \leq -\inf_{f\in \bar{A}} S_\theta(f),$$

where $\bar{A}$ *is the closure of* A, A° *the interior of* A.

REMARK. The non-trivial aspect of this result is to establish the LDP in the uniform convergence topology. We choose to achieve this by arguing that the process $K_n^\theta(t)/\log n$ is exponentially equivalent to the Poisson process.

THEOREM 1.2. *For* $\alpha \in (0,1), \theta + \alpha > 0$, *the sequence* $\{\nu_n^{\alpha,\theta}\}_{n\geq 1}$ *satisfies a large deviation principle with rate function* $I^\alpha(\cdot)$ *and speed* n, *where* $\nu_n^{\alpha,\theta}$ *is the law of* $K_n^{\alpha,\theta}/n$ *under* $P_n^{\alpha,\theta}$.

$$I^\alpha(x) = \sup_\lambda \{\lambda x - \Lambda_\alpha(\lambda)\}, \tag{1.6}$$

and

$$\Lambda_\alpha(\lambda) = \begin{cases} -\log\left[1-(1-e^{-\lambda})^{\frac{1}{\alpha}}\right] & \text{if } \lambda > 0, \\ 0, & \text{otherwise.} \end{cases} \tag{1.7}$$

REMARK. For the Ewens sampling formula ($\alpha = 0, \theta > 0$), let μ_n^θ be the law of $K_n^\theta/\log n$ under P_n^θ in (1.1). Then one can show that the sequence $\{\mu_n^\theta\}_{n\geq 1}$ satisfies a large deviation principle with speed $\log n$ and rate function

$$I_\theta(x) = \begin{cases} x\log\frac{x}{\theta} - x + \theta, & \text{for } x > 0 \\ \theta, & \text{for } x = 0 \\ +\infty, & \text{for } x < 0 \end{cases}$$

by using the representation of K_n^θ as a sum of independent components and the generating function formula for the Stirling Numbers of the first kind.

Our approach involves a result of independent interest by providing a biological basis for Pitman's sampling formula as a particular example of a general class of models introduced in [8], in the same fashion as [14] provides an embedding interpretation of the urn model [7] leading to Ewens sampling formula. This embedding leads to a simple intuitive proof of the existence of $\lim_{n\to\infty} K_n^{\alpha,\theta}/n^\alpha$.

Proofs, as well as further details, will appear in a forthcoming paper by the authors.

2. Embedding. The limiting distribution in (1.5) can be easily understood using an interpretation of (1.2) as the marginal distribution of the embedded jump chain of a continuous time birth-immigration process inspired by [8].

Consider a population comprised of a various number of different types (say mutants) which is evolving continuously in time. Mutants arrive at the times $0 \leq T_1 < T_2 < \cdots$ and initiate independent identically distributed subpopulations. Let $I(t) = \{j : T_j \leq t\}$ be the number of mutant lines which have arrived in $[0,t]$,

$x_i(t-T_i)$ is the size of the i-th mutant line at time t, and $N(t) = \sum_{i=1}^{I(t)} x_i(t-T_i)$ represents the total population size at time t. For the purpose of this paper we assume that $I(0) = 0, x(0) = 1$, and both $I(t)$ and $x(t)$ are pure birth process with respective birth rates r_k and l_k such that $r_0 = \beta_0$, $r_k = \alpha(k-1) + \beta$, $l_k = k - \alpha$ for $k \geq 1$. Here $\beta_0 > 0, \beta > 0$, and $\alpha \in (0,1)$ are arbitrary constants. It follows that $N(t)$ is also a pure birth process with $N(0) = 0$ and birth rate ρ_n such that $\rho_0 = \beta_0$ and $\rho_n = n + \beta - \alpha$ for $n \geq 1$.

The mutant lines induce a random partition $\Pi(t)$ of $N(t)$ given by $m_i(t) = \sharp\{j : T_j \leq t \text{ and } x_j(t-T_j) = i\}$ for $1 \leq i \leq N(t)$ so that $m_i(t)$ is the number of mutant lines with i representatives at time t. For $n \geq 1$ define $\tau_n = \inf\{t \geq 0 : N(t) = n\}$ and consider the random partition $\Pi_n = \Pi(\tau_n)$. We can show that the conditional distribution of Π_{n+1} given Π_n is identical to equation (15) in [11] with notation $\theta = \beta - \alpha$ in place of β. This establishes the following theorem.

THEOREM 2.1. *The distribution of the random partition $\Pi_n(\tau_n)$ is given by the Pitman formula*

$$P[\Pi(\tau_n) = (m_1, \ldots, m_n)] = \frac{n!}{[\theta]^n} \Pi_{l=0}^{k-1}(\theta + l\alpha) \Pi_{j=1}^{n} \frac{\left([1-\alpha]^{j-1}\right)^{m_j}}{(j!)^{m_j}(m_j!)},$$

where $k = \sum_{i=1}^{n} m_i$.

Each of the processes $I(t)$, $x(t)$, and $N(t)$ has structure analogous to a linear birth process with immigration, generically denoted by $Y(t)$, which is a time homogeneous Markov chain with infinitesimal parameter $\lambda_n = \lambda n + c$ with $\lambda > 0, c > 0$. Typically $Y(0) = 0$.

It is known that if $Y(0) = 0$, then

$$\lim_{t\to\infty} e^{-\lambda t} Y(t) = W_{\frac{c}{\lambda}}, \ a.s., \tag{2.1}$$

where W_d has the gamma density

$$f(x) = \frac{e^{-x} x^{d-1}}{\Gamma(d)}, \quad x > 0.$$

Applying (2.1) to $I(t), N(t)$, one gets

$$\lim_{t\to\infty} e^{-\alpha t} I(t) = e^{-\alpha T_1} W_\beta, \ a.s., \tag{2.2}$$

where T_1 and W_β are independent, and T_1 has an exponential distribution with mean β_0^{-1}, and

$$\lim_{t\to\infty} e^{-t} N(t) = e^{-T_1} W_{1+\beta-\alpha}, \ a.s., \tag{2.3}$$

From the ratio of (2.2) and (2.3) we easily obtain the following proof and representation of (1.5) and also an explanation of the factor n^α.

THEOREM 2.2. *For* $0 < \alpha < 1$, $\theta > -\alpha$,

$$\lim_{n\to\infty} \frac{K_n^{\alpha,\theta}}{n^\alpha} = S_{\alpha,\theta} = \frac{W_{\theta+\alpha}}{(W_{1+\theta})^\alpha}, \ a.s. \tag{2.4}$$

which implies that $P[0 < S_{\alpha,\theta} < \infty] = 1$.

REMARK. The main novelty of the embedding in this section is that the immigration of mutants is not Poisson (as in the Ewens case) but is a pure birth process itself. Moreover each mutant line does not behave according to binary splitting (which would require $l_n = n, n \geq 1$ rather than $l_n = n - \alpha$, as is the case).

3. Sketch of Proofs.

PROOF OF THEOREM 1.1. Since $\alpha = 0$, the pure birth process $I(t)$ introduced in Section 2 is now a homogeneous Poisson process with parameter $\theta > 0$. Let

$$\bar{K}_n(t) = \sum_{k=1}^{I(\tau_n)} I_{\{x_k(\tau_n - T_k) \leq n^t\}}.$$

Since $K_n^\theta(t)$ and $\bar{K}_n(t)$ have the same law it suffices to verify the result for the sequence $\{\bar{K}_n(t)/\log n\}_{n\geq 1}$. In a series of lemmas we are able to show that $\{\bar{K}_n(t)/\log n\}$ is exponentially equivalent to $\frac{I((\log n)t+(\log n)^\delta)}{\log n}$ for $\delta \in (0, 1/2)$. Finally applying the following Theorem 3.1 one gets the result. ∎

THEOREM 3.1. *Let* $\{b_n\}_{n\geq 1}$ *a sequence of positive numbers such that* $\lim_{n\to\infty} b_n/a_n = 0$. *Let* $Z_n(t) = \frac{I(a_n t + b_n)}{a_n}$ *and* Q_n *be the law of* $Z_n(t)$ *on space* $\mathbf{D}[0,1]$. *Then the sequence* $\{Q_n\}_{n\geq 1}$ *satisfies a large deviation principle on space* $\mathbf{D}[0,1]$ *with rate function* $S(\cdot)$ *and speed* a_n.

PROOF OF THEOREM 1.2. The main part in the proof of Theorem 1.2 is to show that

$$\lim_{n\to\infty} \frac{1}{n} \log E[e^{\lambda K_n^{\alpha,\theta}}] = \Lambda_\alpha(\lambda),$$

which involves some complicated combinatorial arguments. This, combined with the facts that $\{\lambda\ ;\ \Lambda_\alpha(\lambda) < \infty\} = R$, $\Lambda_\alpha(\lambda)$ is differentiable, and Theorem 2.3.6 (Gärtner-Ellis theorem) in [3], implies the result. ∎

REFERENCES

1. C. Antoniak, *Mixtures of Dirichlet processes with applications to Bayesian nonparametric problems.* Ann. Statist. **2**(1974), 1152–1174.
2. J. M. DeLaurentis and B. G. Pittel, *Random permutations and Brownian motion.* Pacific J. Math. **119**(1985), 287–301.
3. A. Dembo and O. Zeitouni, *Large Deviations and Applications.* Jones and Bartlett Publishers, Boston, 1993.
4. W. J. Ewens, *The sampling theory of selectively neutral alleles.* Theoret. Population Biol. **3**(1972), 87–112.

5. V. L. Goncharov, *Some facts from combinatorics.* IZV. Akad. Nauk. SSSR, Ser. Mat. **8**(1944), 3–48.
6. J. C. Hansen, *A functional central limit theorem for the Ewens sampling formula.* J. Appl. Probab. **27**(1990), 28–43.
7. F. M. Hoppe, *Pólya-like urns and the Ewens sampling formula.* J. Math. Biol. **20**(1984), 91–94.
8. S. Karlin and J. McGregor, *The number of mutant forms maintained in a population.* Proc. Fifth Berkely Symp. Math. Statist. and Prob. (Eds. L. LeCam and J. Neyman), 1967, 415–438.
9. J. F. C. Kingman, *Random partitions in population genetics.* Proc. Roy. Soc. London Ser. A **361**(1978), 1–20.
10. J. Pitman, *The two parameter generalization of the Ewens random partition structure.* Unpublished note, 1992.
11. ———, *Exchangeable and partially exchangeable random partitions.* Probab. Theory Related Fields **102**(1995), 145–158.
12. ———, *Partition structures derived from Brownian motion and stable subordinators.* Technical Report **346**, Dept. Statistics, U.C. Berkeley. To appear in Bernoulli.
13. L. A. Shepp and S. P. Lloyd, *Ordered cycle lengths in a random permutation.* Trans. Amer. Math. Soc. **121**(1966), 340–357.
14. S. Tavaré, *The birth process with immigration and the genealogical structure of large populations.* J. Math. Biol. **25**(1987), 161–168.

Department of Mathematics and Statistics
McMaster University
Hamilton, Ontario
L8S 4K1
email: shuifeng@mcmail.cis.mcmaster.ca
hoppe@mcmail.cis.mcmaster.ca

C. R. Math. Rep. Acad. Sci. Canada Vol. **20** (3), 1998 pp. 71–76

EXACT RATIONAL SOLUTIONS OF A TRANSCENDENTAL EQUATION

D. J. JEFFREY, D. E. G. HARE AND R. M. CORLESS

Presented by J. M. Borwein, FRSC

ABSTRACT. The equation $x^n b^x = c$ is solved using the Lambert W function. A new simplification rule for W is given that allows those cases in which the equation has rational solutions for x to be identified. A related equation studied by Euler, $x^y = y^x$, is also investigated using W.

RÉSUMÉ. On résout l'équation $x^n b^x = c$ en utilisant la fonction W de Lambert. Une nouvelle règle de simplification pour W est donnée qui permet d'identifier et de calculer certains cas pour lesquels l'équation possède des solutions rationnelles x. Nous examinons aussi à l'aide de la fonction W une équation apparentée à la première et qui fut étudiée par Euler, $x^y = y^x$.

1. Introduction.

For $n \in \mathbb{Z}$, $b, c \in \mathbb{Q}$ and $b > 0$, the equation

$$x^n b^x = c \tag{1}$$

has, in general, solutions $x \in \mathbb{C}$. The most interesting cases, however, usually have some solutions $x \in \mathbb{Q}$, and a method is needed to find both types of solution. The general solution of (1) is obtained below in terms of the Lambert W function $W_k(z)$, which is defined by [1]

$$W_k(z) e^{W_k(z)} = z, \tag{2}$$

where k identifies the branch of this multivalued inverse function. Thus an automatic solution of (1) by computer is possible, except for the difficulty of identifying rational solutions. Consider $x^2 2^x = 72$, which has an infinite number of non-rational solutions, and the solution $x = 3$. In terms of W, this solution is

$$x = \frac{2}{\ln 2} W_0\left(3\sqrt{2}\ln 2\right),$$

which implies the simplification $W_0\left(3\sqrt{2}\ln 2\right) = (3/2)\ln 2$, but no rule covering this has been previously reported. Such simplification rules must be investigated before equation (1) can be solved in the best way. In addition, new simplifications may prove useful in other applications of the Lambert W function.

Received by the editors October 13, 1997.
AMS subject classification: 11-04, 26-04, 33E99, 65H05.

2. Real solutions and rational solutions. In (1), the case $b < 1$ can be avoided by the transformation $x \to -x$, so only the case $b > 1$ is considered.

THEOREM 1. *Let $b, c \in \mathbb{R}$, $b > 1$ and $n \in \mathbb{Z}$. Let $\sqrt[n]{c}$ denote the real branch of $c^{1/n}$. The solutions $x \in \mathbb{R}$ of the equation $x^n b^x = c$ are as follows.*

1. *If n is odd and $c > -(n/e \ln b)^n$ or if n is even and $c \geq 0$,*

$$x = \frac{n}{\ln b} W_0\left(\frac{\ln b}{n} \sqrt[n]{c}\right).$$

2. *If n is odd and $0 > c > -(n/e \ln b)^n$,*

$$x = \frac{n}{\ln b} W_{-1}\left(\frac{\ln b}{n} \sqrt[n]{c}\right).$$

3. *If n is even and $0 < c \leq (n/e \ln b)^n$,*

$$x = \frac{n}{\ln b} W_0\left(-\frac{\ln b}{n} \sqrt[n]{c}\right), \quad \text{or} \quad x = \frac{n}{\ln b} W_{-1}\left(-\frac{\ln b}{n} \sqrt[n]{c}\right).$$

PROOF. Consider the case for n odd. Take the real-branch n-th root of both sides of (1). Then it becomes, because n is odd,

$$x b^{x/n} = x e^{(x/n) \ln b} = \sqrt[n]{c},$$

and multiplying through by $(\ln b)/n$ and comparing with (2) establishes that

$$x = \frac{n}{\ln b} W_k\left(\frac{\ln b}{n} \sqrt[n]{c}\right).$$

Only the branches $k = 0$ and $k = -1$ of W take real values [1]. The principal branch $W_0(x)$ is real for $x \geq -1/e$, while $W_{-1}(x)$ is real for $-1/e < x < 0$. Imposing these restrictions leads to the cases listed in the theorem. The other cases are similar. It is clear that the converse statements are also true.

EXAMPLE. The solutions of $x^2(9/16)^x = 3/16$ are

$$\frac{-2}{\ln(16/9)} W_0\left(\frac{\sqrt{3}}{8} \ln \frac{16}{9}\right) \approx -.387351650,$$

$$\frac{-2}{\ln(16/9)} W_0\left(-\frac{\sqrt{3}}{8} \ln \frac{16}{9}\right) = \frac{1}{2},$$

$$\frac{-2}{\ln(16/9)} W_{-1}\left(-\frac{\sqrt{3}}{8} \ln \frac{16}{9}\right) \approx 11.35508246.$$

One must be aware of the possibility of equivalent expressions:

$$\frac{-2}{\ln(16/9)} W_0\left(-\frac{\sqrt{3}}{8} \ln \frac{16}{9}\right) = \frac{-1}{\ln(4/3)} W_0\left(-\frac{\sqrt{3}}{4} \ln \frac{4}{3}\right) = \frac{1}{2}.$$

We are led by the above to seek an algorithm for deciding whether $W_k(r_1 \sqrt[n]{r_2} \ln b)$, with $r_1, r_2, b \in \mathbb{Q}$, simplifies to $r \ln b$, with $r \in \mathbb{Q}$. A standard method for obtaining rational numbers from approximate data is to truncate a continued-fraction expansion [5], and therefore the obvious strategy is to evaluate $W/\ln b$ as a floating point number and then to expand the result as a continued fraction. This idea has two drawbacks, and they are related: first, the number of digits at which the computation is done will determine its success, and second, it is not a decision procedure, because failure to find a rational simplification is no proof that one does not exist. For example, consider the following problem, worked first using 10 digits.

$$W_0\left(\frac{528309}{168976} \ln\left(\frac{9}{4}\right) 3^{\frac{7451}{10561}} 2^{\frac{3110}{10561}}\right) \Big/ \ln\frac{9}{4} \approx 1.852760155. \tag{3}$$

The continued-fraction expansion, in the notation of [5], begins

$$1.852760155 \approx [1, 1, 5, 1, 3, 1, 3, 1, 63, 1, 30].$$

Re-computed using 16 digits, the continued fraction becomes

$$1.852760155288325 \approx [1, 1, 5, 1, 3, 1, 3, 1, 64, 291347701].$$

Therefore, it is only at 16 digits of precision that we are led to conjecture, correctly, that $r = [1, 1, 5, 1, 3, 1, 3, 1, 64]$; in other words

$$W_0\left(\frac{528309}{168976} \ln\left(\frac{9}{4}\right) 3^{\frac{7451}{10561}} 2^{\frac{3110}{10561}}\right) = \frac{19567}{10561} \ln\frac{9}{4}.$$

If this method fails, it might be that no rational simplification exists, or it might be merely that the precision used was insufficient. An algorithm that guarantees a decision is based on the following definition and theorem.

DEFINITION. The integer power content of $b \in \mathbb{Q}$ is the largest $m \in \mathbb{Z}$ such that $b = \hat{b}^m$ and $\hat{b} \in \mathbb{Q}$. We write $m = \operatorname{ipc} b$, and call $\hat{b}$ the integer-power-free reduction of b, written $\hat{b} = \operatorname{ipf} b$. Clearly $b = (\operatorname{ipf} b)^{\operatorname{ipc} b}$.

THEOREM 2. *Given $r_1, r_2, b \in \mathbb{Q}$, the simplification of $W_k(r_1 \sqrt[n]{r_2} \ln b)$ to the form $r \ln b$, with $r \in \mathbb{Q}$, is possible if and only if $k = 0$ or $k = -1$ and*

$$x = \frac{n}{\ln(\operatorname{ipf} b)} W_k(r_1 \sqrt[n]{r_2} \ln b) \in \mathbb{Z}, \tag{4}$$

in which case $r = x \operatorname{ipc}(b)/n$. Moreover, x is an integral solution of

$$(\operatorname{ipf} b)^x - \left(\frac{r_1 n \operatorname{ipc} b}{x}\right)^n r_2 = 0. \tag{5}$$

PROOF. By theorem 1, x as defined in (4) is a solution of

$$x^n(\mathrm{ipf}\, b)^x = c = r_1^n n^n (\mathrm{ipc}\, b)^n r_2. \tag{6}$$

Then $x \in \mathbb{Q} \Rightarrow x \in \mathbb{Z}$, because if $x = p/q$, with $p, q \in \mathbb{Z}$, then

$$(\mathrm{ipf}\, b^p)^{1/q} = c(q/p)^n.$$

Clearly the right-hand side is rational, but by the construction of $\mathrm{ipf}\, b$, the left side is not in $\mathbb{Q}$ unless $q = 1$.

Computational algorithm. A practical procedure is as follows. The quantity x defined in (4) is evaluated in two stages. At first, the order of magnitude of x is determined; let it be $O(10^p)$. The evaluation is then repeated using more digits of precision than p, so that if x is indeed an integer, its value will be determined correctly.[1] The proposed integral value is then accepted if it satisfies (5), otherwise there is no rational simplification. If a computer system verifies (5) by direct computation of the left-hand side, very large integers are generated. It would therefore be wise for a system to use the laws of exponents first.

EXAMPLE. Returning to problem (3), one now computes

$$\frac{10561}{\ln(3/2)} W_0\left(\frac{528309}{168976}\ln\left(\frac{9}{4}\right) 3^{\frac{7451}{10561}} 2^{\frac{3110}{10561}}\right) \approx 39135.$$

where 5 digits of precision have been used. The size of the result shows that a computation accurate to 6 digits is sufficient (less than half the 16 needed by the continued fraction method), and this gives 39134.0 as the result. We now must verify that

$$(3/2)^{39134} - \left(\frac{528309}{168976}\frac{(10561)2}{39134}\right)^{10561} 3^{7451}2^{3110} = 0.$$

A brute-force evaluation of the left-hand side takes about 20 seconds on existing computers, but working in powers of 2 and 3 gives rapid verification.

3. A problem solved by Euler. An interesting related equation was studied by Euler and others, namely,

$$x^y = y^x.$$

Regarding y as a given quantity makes this equation a special case of (1). For $x > 0$ and $y > 0$ it is straightforward to obtain the solution $x = -yW_k(-\ln y/y)/\ln y$. In addition to the solution $x = y$, the equation has the parametric solutions

$$x = (1+s)^{1/s}, \qquad y = (1+s)^{1+1/s},$$

[1] Arithmetic in Maple V release 5 is guaranteed to produce results accurate to 0.6 ulp for fundamental operations such as multiplication and single function evaluations. Other systems are similar. Evaluation of a simple composition of these operations, such as $aW(b\ln c)$ for numeric a, b and c, can be proved accurate—with some work—if enough guard digits are used in the computation.

and the symmetric solution (y,x). This implies simplification rules for W. We find from the $y = x$ solution, setting $y = 1/t$,

$$W_0(t\ln t) = \ln t, \quad \text{for} \quad t > 1/e,$$
$$W_{-1}(t\ln t) = \ln t, \quad \text{for} \quad 0 < t < 1/e.$$

From the parametric solution, we obtain the additional relations

$$W_0\left(-\frac{\ln(1+s)}{s(1+s)^{1/s}}\right) = -\frac{1+s}{s}\ln(1+s) \quad \text{for } -1 < s < 0,$$
$$W_{-1}\left(-\frac{\ln(1+s)}{s(1+s)^{1/s}}\right) = -\frac{1+s}{s}\ln(1+s) \quad \text{for } 0 < s.$$

These results are equivalent to a result by Lauwerier [3, 4]. Equations (54–57) in [3] are obtained by writing $s = e^{2\Delta} - 1$. As of this writing, there are no computer algebra implementations of these (domain-specific) simplification rules.

4. The complex case. If all variables are allowed to be complex, then Theorem 1 can be generalized, but without the same degree of completeness. If it is assumed that z^α and b^z are the principal complex values of the power function, we give a formula that generates all solutions of $z^\alpha b^z = c$, but in addition generates solutions that correspond to other branches of the power function. Theorem 3 uses the unwinding number $\mathcal{K}$, but defined as the negative of the unwinding number defined in [2]. Thus, it is now defined for $z \in \mathbb{C}$ as

$$\ln e^z = z - 2\pi i\mathcal{K}(z). \tag{7}$$

After working with $\mathcal{K}$, it has become clear to us that this new definition is better, because fewer minus signs arise in the equations.

THEOREM 3. *Let $\alpha, b, c \in \mathbb{C}$. If $z \in \mathbb{C}$ is a solution of $z^\alpha b^z = c$, then it satisfies*

$$z = \frac{\alpha}{\ln b} W_k\left(\frac{\ln b}{\alpha} c^{1/\alpha} \exp\left[\frac{2\pi i}{\alpha}\mathcal{K}(\alpha\ln z + z\ln b)\right]\right), \tag{8}$$

where k is any integer and $\mathcal{K}$ is the unwinding number.

PROOF. Take the $1/\alpha$ power of both sides:

$$(z^\alpha b^z)^{1/\alpha} = c^{1/\alpha},$$

where all powers are principal value. In terms of the unwinding number,

$$(z^\alpha b^z)^{1/\alpha} = z b^{z/\alpha} \exp\left(-\frac{2\pi i}{\alpha}\mathcal{K}(\alpha\ln z + z\ln b)\right).$$

The solution of the equation then follows as stated.

The theorem can be used algorithmically to generate solutions for $z^\alpha b^z = c$, by taking advantage of the fact that both k and $\mathcal{K}$ are integers. Stepping through the ranges of k and $\mathcal{K}$ generates all possible solutions, and some spurious solutions. Each new solution must to be verified in the original equation.

EXAMPLE. For the equation $x^{1/3}256^x = 1$, the exponential factor in (8) is 1, but even so, W_0 and W_3 give solutions, but W_{-1}, W_1, W_2 do not, unless $x^{1/3}$ takes values from its other branches.

REFERENCES

1. Robert M. Corless, G. H. Gonnet, D. E. G. Hare, D. J. Jeffrey and D. E. Knuth, *On the Lambert W Function*. Adv. Comput. Math. **5**(1996), 329–359.
2. Robert M. Corless and D. J. Jeffrey, *The unwinding number*. SIGSAM Bulletin **30**(1996), 28–35.
3. Robert M. Corless, D. J. Jeffrey and D. E. Knuth, *A sequence of series for the Lambert W function*. In: Proceedings of ISSAC '97, ACM Press, 1997, 197–204.
4. H. A. Lauwerier, *The asymptotic expansion of the statistical distribution of N. V. Smirnov*. Z. Wahrscheinlichkeitstheorie **2**(1963), 61–68.
5. C. D. Olds, *Continued fractions*. Mathematical Association of America, Washington, DC, 1963.

Department of Applied Mathematics
The University of Western Ontario
London, Ontario
N6A 5B7
email: Robert.Corless@uwo.ca; djj@uwo.ca

Symbolic Computation Group
Computer Science Department
University of Waterloo
Waterloo, Ontario
email: deghare@daisy.uwaterloo.ca

C. R. Math. Rep. Acad. Sci. Canada Vol. **20** (3), 1998 pp. 77–82

CONGRUENCES FOR THE SPECIAL VALUES OF MODULAR L-FUNCTIONS

V. VATSAL

Presented by M. Ram Murty, FRSC

ABSTRACT. The results of this note show how congruences between the Fourier coefficients of modular forms give rise in a general setting to congruences between the critical values of the associated L-functions. Let E be an elliptic curve over $\mathbb{Q}$ with a rational point of order three, and of good reduction at three. Let χ_D denote the character of an imaginary quadratic field. We use our results to show that the twisted curves $E \otimes \chi_D$ often have rank zero.

RÉSUMÉ. Les résultats de cette note montrent comment les congruences entre les coefficients de Fourier des formes modulaires permettent d'obtenir dans un cadre général des congruences entre les valeurs critiques des fonctions L associées. Soit E une courbe elliptique sur $\mathbb{Q}$ ayant un point rationnel d'ordre trois et ayant bonne réduction en trois. Notons par χ_D le caractère d'un corps quadratique complexe. Nous utilisons nos résultats pour montrer que les valeurs speciales tordues $L(1, E \otimes \chi_D)$ sont souvent non-nulles.

The purpose of this announcement is to describe some results which state, roughly, that a congruence between modular forms gives rise to a congruence between L-values. This phenomenon fits in with general algebraic arguments from Iwasawa theory, where one considers representations and Selmer groups instead of modular forms and L-values. As has become evident in light of recent work by Ono-Skinner [OSa], [OSb], James, and Kohnen [Koh97], such congruences are a useful tool in proving nonvanishing theorems. Our results continue this trend, and we obtain a new nonvanishing theorem for the L-functions of elliptic curves with a rational point of order three. This generalizes an example due to Kevin James, and provides new evidence for a conjecture of Goldfeld [Gol79] on the ranks of elliptic curves in families of quadratic twists. The proofs of the results stated in this article will appear in our forthcoming article [Vat97].

We want to begin by discussing the general facts about congruences. Thus let $f = \sum a_n q^n$ be an cuspform of level $M \geq 4$ and weight $k \geq 2$. Since $M \geq 4$, we see that the group $\Gamma = \Gamma_1(M)$ is torsion-free. Assume that f is a simultaneous eigenform for all the Hecke operators and that $a_1(f) = 1$. The L-function associated to f is defined by the Dirichlet series $L(s, f) = \sum a_n n^{-s}$, which converges

Received by the editors November 27, 1997.
AMS subject classification: 11F67.

for $\mathrm{Re}(s) > \frac{k+1}{s}$ and has analytic continuation to $s \in \mathbb{C}$. A fundamental theorem of Shimura [Shi76] states that $L(s,f)$ enjoys the following algebraicity property:

THEOREM 1.1 (SHIMURA). *There exist complex periods $\Omega_f^{\pm}$ such that, for each integer m satisfying $0 \leq m \leq k-2$, and every Dirichlet character χ, the quantity*

$$\tau(\overline{\chi}) \cdot m! \frac{L(m+1,f,\chi)}{(-2\pi i)^{m+1}\Omega_f^{\pm}}$$

is algebraic. Here the sign $\pm$ of $\Omega^{\pm}$ is determined by $\pm 1 = \chi(-1)$, and $\tau(\overline{\chi})$ denotes the Gauss sum attached to $\overline{\chi}$.

The integers m appearing in Shimura's theorem are said to be *critical* for $L(s,f)$.

Now consider another eigenform $g = \sum b_n q^n$, where the Fourier coefficients b_n are related to those of f by a congruence:

$$a_n \equiv b_n \pmod{\mathfrak{p}},$$

for a prime ideal $\mathfrak{p}$ in the ring of all algebraic integers (we need to fix an embedding of the algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$ into $\mathbb{C}$). Then general arguments from Iwasawa theory [BK90], [Coa91], [Gre89], suggest that algebraic parts of special values should reflect algebraic properties, so that for critical m, there should be a congruence

$$\tau(\overline{\chi}) \cdot m! \frac{L(m+1,f,\chi)}{(-2\pi i)^{m+1}\Omega_f^{\pm}} \equiv \tau(\overline{\chi}) \cdot m! \frac{L(m+1,g,\chi)}{(-2\pi i)^{m+1}\Omega_g^{\pm}} \pmod{\mathfrak{p}}. \tag{1}$$

Of course the crucial ingredient in proving such congruences is the determination of the periods $\Omega_*^{\pm}$, since Shimura's theorem only specifies them up to an algebraic constant. A related question arises in the definition of p-adic L-functions in Iwasawa theory, where one needs to specify these periods up to p-adic unit [Gre89], [Coa91]. Partial results in this direction have been obtained by a number of authors [AS86], [Maz79], [Ste82], but we are able to subsume all these into a rather general framework. In fact, we can show that *all* such congruences can be derived formally from a sufficiently precise description of the Hecke-module structure of the cohomology with coefficients of the appropriate modular curves. The condition we need can be stated as follows:
There exists an isomorphism of Hecke modules

$$\theta : H^1_{\mathrm{par}}(\Gamma, L_n(\mathbb{Z}_p))_{\mathfrak{m}} \cong \left(S_k(\Gamma, \mathbb{Z}_p)_{\mathfrak{m}}\right)^2. \tag{2}$$

Here $H^1_{\mathrm{par}}(\Gamma, L_n(\mathbb{Z}_p)$ denotes the Eichler-Shimura parabolic group cohomology module of degree $n = k-2$, and $S_k(\Gamma, \mathbb{Z}_p)$ denotes the space of (classical) cusp-forms for Γ with coefficients in $\mathbb{Z}_p$. The subscript $\mathfrak{m}$ denotes localization at the

appropriate maximal ideal in the Hecke ring. The condition (2) is closely related to the 'multiplicity one' theorems of Mazur, Ribet, Wiles, and others, and can be verified under some hypotheses. For example we have the following concrete result:

THEOREM 1.2. *Let p be an odd prime, and let $f = \sum a_n q^n$ and $g = b_n q^n$ be cuspidal newforms of weight k on $\Gamma_1(M)$, such that $a_n \equiv b_n \pmod{\mathfrak{p}^r}$, for some prime $\mathfrak{p}$ above p in $\overline{\mathbb{Q}}$. Assume that the mod $\mathfrak{m}$ reprentation $\overline{\rho}$ attached to F is irreducible, as well as either one of the following conditions:*

- *$(M, p) = 1$ and that $p > k$, or*
- *$\overline{\rho}$ is ordinary and p-distinguished.*

Fix an isomorphism $\mathbb{C}_p \cong \mathbb{C}$, such that the prime $\mathfrak{p}$ of $\overline{\mathbb{Q}} \subset \mathbb{C}$ induces the usual absolute value on $\mathbb{C}_p$. Then there exist canonical periods $\Omega_f^{\pm}$ and $\Omega_g^{\pm}$ such that the congruence (1) holds modulo $\mathfrak{p}^r$, for every character χ.

REMARK 1.3. We remind the reader that the representation $\overline{\rho}$ is said to be p-distinguished if its restriction to a decomposition group D_p admits an unramified quotient of rank 1, and the Jordan-Holder factors on D_p are distinct.

The proof of the theorem is a direct application of the theory of modular symbols. Assume for simplicity that f and g have rational Fourier coefficients. Then one decomposes the isomorphism in (2) according to the action of complex conjugation to obtain isomorphisms

$$\theta^{\pm} : H^1_{\mathrm{par}}(\Gamma, L_n(\mathbb{Z}_p))_{\mathfrak{m}} \cong S_k(\mathbb{Z}_p)_{\mathfrak{m}};$$

this permits us to define canonical coholomology classes $\delta_*^{\pm} = \theta^{\pm}(*) \in H^1_{\mathrm{par}}(\Gamma, \mathbb{Z}_p)$, for $* = f$ or $* = g$. The congruences between f and g give congruences between $\delta_f^{\pm}$ and $\delta_g^{\pm}$, and hence between the associated modular symbols. The key hypothesis is the irreducibility of the residual representation $\overline{\rho}$, which not only intervenes in the verification of (2) but also allows us to identify modular symbols with group cohomology classes. We refer the reader to [GS93] for a discussion of the general theory of modular symbols and for the connection of the modular symbols with L-values.

One can still salvage something when the residual representation is reducible, but the results are less satisfactory as the Hecke-module structure of the cohomology is not well-understood, and isomorphisms like (2) are not known in general. One has therefore to seek out another condition. Nevertheless, a considerable amount can be retrieved, and results analogous to (1.2) are obtained. A precise statement is somewhat complicated, and we refer the reader to our forthcoming article [Vat97].

Finally, our method yields a refinement of an old result due to Mazur and Stevens [Maz79], [Ste82], which states that the L-values of a weight-two cuspform whose Fourier coefficients are congruent to those of an Eisenstein series has the property that its L-values are congruent to certain products of Bernoulli numbers:

THEOREM 1.4. *Let $f = \sum a_n(f)q^n$ be a cuspform on Γ, of weight two, and let $E = \sum a_n(E)q^n$ be an Eisenstein series. Assume that*

- *f and E are eigenforms for all the Hecke operators,*
- *$a_n(f) \equiv a_n(E) \pmod{\mathfrak{p}^r}$, for $n \geq 1$ and a prime $\mathfrak{p}$ above the odd prime p,*
- *the constant terms of E at all cusps of Γ are all divisible by $\mathfrak{p}^r$, and*
- *$(M, p) = 1$.*

Then there exists periods Ω_f and Ω_E such that

$$\tau(\overline{\chi})\frac{L(1, f, \chi)}{(-2\pi i)\Omega_f} \equiv \tau(\overline{\chi})\frac{L(1, E, \chi)}{(-2\pi i)\Omega_E} \pmod{\mathfrak{p}^r},$$

for all characters χ of conductor prime to p and fixed parity $\epsilon(E)$. Here the sign $\epsilon(E)$ may be determined as $\epsilon(E) = -\psi_1(-1)$, where the character ψ_1 is defined by $L(s, E) = L(s, \psi_1) \cdot L(s-1, \psi_2)$.

The proof of this theorem is very similar to the original arguments of Mazur and Stevens. However, our formulation yields a slightly stronger result and requires no study of the cuspidal group.

2. Application to nonvanishing theorems. Let f be a modular cuspform even weight $k = 2m$. Let D be a square-free integer, and let χ_D denote the Kronecker character associated to the quadratic field $\mathbb{Q}(\sqrt{D})$. For a positive real number X, define the number

$$M_f(X) = \#\{D : |D| < X,\ L(m, f \otimes \chi_D) \neq 0\}.$$

Then a well-known conjecture in analytic number theory states that $M_f(X) \gg X$. There are a number of partial results in this direction, due to Murty-Murty [MM91], Iwaniec [Iwa90], and others; currently the best estimate is due to Ono and Skinner [OSb] who prove that $M_f(X) \gg X/\log(X)$.

In the case where f has weight 2 and corresponds to an elliptic curve over $\mathbb{Q}$, Goldfeld has conjectured that $M_f(X) \sim X/2$ (see [Gol79] for a more precise statement). A recent example due to Kevin James [Jam] shows that $M_f(X) \gg X$ for a certain modular elliptic curve of level 14. Our final result extends James' ideas to yield the following theorem:

THEOREM 2.1. *Let E be a modular elliptic curve over $\mathbb{Q}$ with a rational point of order three. Assume that E has good ordinary reduction at 3, and that the conductor N of E is square-free. Let f be the newform associated to E. Then $M_f(X) \gg X$.*

The proof of the theorem is based on a mod 3 relationship between the algebraic part of $L(1, E \otimes \chi_D)$ and the class-number of the field $\mathbb{Q}(\sqrt{D})$, which follows from the general congruence machinery (in fact, from the Mazur-Stevens theorem). The estimate on $M_f(X)$ then follows from a theorem of Davenport and Heilbronn, as refined by Nakagawa and Horie [NH88]. This application of

the Davenport-Heilbronn theorem is due to James, whose original work gave a version of our theorem for a the curve 14B in Cremona's tables. It should be pointed out that James relates the L-values to class numbers by using Waldspurger's theorem and the Shimura lift, rather than the theory of congruences. His technique has also been exploited by Kohnen [Koh97] to obtain nonvanishing results for certain forms of level 1, including the Ramanujan Δ-function.

We briefly decribe the congruence between the Eisenstein series and the curve E which allows us to relate the L-values to class numbers. Let q be a prime of good reduction for E. Let n_q denote the number of points on E modulo q. Then $a_q = n_q - q + 1$ is the q-th Fourier coefficient of the modular form associated to E. The existence of the 3-torsion point on E implies that, for a prime $q \neq 3$ that we have

$$3|n_q \Longrightarrow a_q \equiv q + 1 \pmod 3.$$

But now recall that $q + 1 = \sum_{d|q} d = \sigma_1(q)$ is the q-th Fourier coefficient of the (non-holomorphic) Eisenstein series $G(z)$ of level 1 and weight 2. The L-series of G is $L(s, G) = \zeta(s) \cdot \zeta(s-1)$, so that, for an odd quadratic character χ_D, we have $L(s, G) \otimes \chi_D = L(s, \chi_D) \cdot L(s-1, \chi_D)$. Thus we expect a congruence between $L(1, E \otimes \chi_D)$ and $L(1, \chi_D) \cdot L(0, \chi_D)$, at least up to Euler factors at the bad primes. In view of the functional equation and the classical class number formula, we find, if χ_D is odd, that $L(1, G \otimes \chi_D)$ is equal to $h(D)^2$ up to the appropriate period, for the class number $h(D)$ of $\mathbb{Q}(\sqrt{D})$. The Mazur theorem allows us to make this heuristic argument precise; we refer the reader to [Vat97], Section 3 for the details.

REFERENCES

[AS86] A. Ash and G. Stevens, *Modular forms in characteristic ℓ and special values of their L-functions.* Duke Math. J. (3) **53**(1986), 849–868.

[BK90] S. Bloch and K. Kato, *L-functions and the Tamagawa numbers of motives.* In: Grothendieck Festschrift (Eds. P. Cartier *et al.*), Volume 1. Birkhauser, 1990.

[Coa91] J. Coates, *p-adic L-functions.* In: L-Functions and Arithmetic (Eds. J. Coates and M. Taylor). Cambridge University Press, 1991.

[Gol79] D. Goldfeld, *Conjectures on elliptic curves over quadratic fields.* In: Number Theory, Carbondale 1979. Lecture Notes in Math. **751**(1979), 108–118.

[Gre89] R. Greenberg, *Iwasawa theory for p-adic representations.* Adv. Stud. Pure Math. **17**, Amer. Math. Soc., 1989.

[GS93] R. Greenberg and G. Stevens, *p-adic L-functions and p-adic periods of modular forms.* Invent. Math. **111**(1993), 407–447.

[Iwa90] H. Iwaniec, *On the order of nonvanishing of L-functions at the critical point.* Sem. Théor. Nombres Bordeaux **2**(1990), 365–376.

[Jam] K. James, *L-series with nonzero central critical value.* Preprint.

[Koh97] W. Kohnen, *Nonvanishing of Hecke L-functions in the critical strip.* Preprint, 1997.

[Maz79] B. Mazur, *On the arithmetic of special values of L-functions.* Invent. Math. **55**(1979), 207–240.

[MM91] M. R. Murty and V. K. Murty, *Mean values of derivatives of modular L-series.* Ann. Math. **133**(1991), 447–475.

[NH88] J. Nakagawa and K. Horie, *Elliptic curves with no torsion points.* Proc. Amer. Math. Soc. **104**(1988), 20–25.

[OSa] K. Ono and C. Skinner, *Fourier coefficients of half-integer weight forms modulo ℓ.* Preprint.

[OSb] K. Ono and C. Skinner, *Nonvanishing of quadratic twists of modular l-functions.* Preprint.

[Shi76] G. Shimura, *The special values of zeta functions associated with cusp forms.* Comm. Pure Appl. Math. **29**(1976), 783–804.

[Ste82] G. Stevens, *Arithmetic on modular curves.* Progress. Math. **20**. Birkhauser, 1982.

[Vat97] V. Vatsal, *Canonical periods and congruence formulae.* Preprint, 1997.

University of Toronto
vatsal@math.toronto.edu

C. R. Math. Rep. Acad. Sci. Canada Vol. **20** (3), 1998 pp. 83–85

GOLDBACH'S CONJECTURE FOR Z[x]

A. RATTAN AND C. STEWART

Presented by M. Ram Murty, FRSC

ABSTRACT. We use Eisenstein's Criterion to give an elementary proof of an analogue for $\mathbf{Z}[x]$ of Goldbach's Conjecture; namely that any polynomial in $\mathbf{Z}[x]$ can be expressed as the sum of two irreducibles. By a similar technique, we also show that there exist infinitely many $p(x) \in \mathbf{Z}[x]$ such that $p(x)^2 + 1$ is irreducible.

RÉSUMÉ. Nous utilisons le Criterium d'Eisenstein pour donner une preuve élémentaire d'une analogie pour $\mathbf{Z}[x]$ du problème de Goldbach; nommément qu'on peut écrire chaque polynôme dans $\mathbf{Z}[x]$ comme la somme de deux polynômes irréducibles. Par une technique similaire, nous montrons aussi qu'il y a un nombre infini de $p(x) \in \mathbf{Z}[x]$ pour que $p(x)^2 + 1$ est irréducible.

The Goldbach problem, now over 250 years old, has justly become famous for its extreme simplicity of expression as contrasted with the extreme difficulty of finding its solution. In recent years, interest has grown around an analogue of this problem for polynomials over finite fields. We refer the reader to [EH] for a detailed discussion of current techniques to approach this polynomial analogue. Here we consider the problem over $\mathbb{Z}[x]$, with a slight variation from the problem posed in [EH]. Whereas Effinger and Hayes ask when a monic polynomial can be expressed as the sum of two monic irreducibles, we drop the requirement that the polynomials be monic. Before proving the main result we need the following lemma:

LEMMA 1. *Given two distinct odd primes p and q there exist integers r and s such that $rp + sq = 1$ and $p \nmid r$ and $q \nmid s$.*

PROOF. Consider the simultaneous congruences $rp \equiv 1 \pmod{q}$ and $r \equiv 1 \pmod{p}$. By the Chinese remainder theorem, there exists a solution for r to these congruences, *i.e.*, there exist integers r', s' such that $r'p + s'q = 1$ and $p \nmid r'$. Similarly, there exist integers r'', s'' such that $r''p + s''q = 1$ and $q \nmid s''$. If $q \nmid s'$ or $p \nmid r''$ then we are done. Otherwise $p \mid r''$ and $q \mid s'$. Notice that $2(r'p + s'q) - (r''p + s''q) = 1 \Longrightarrow (2r' - r'')p + (2s' - s'')q = 1$. Since $p \nmid r'$,

Received by the editors December 1, 1997.

The authors would like to thank Dr. M. R. Murty for his invaluable suggestions, and M. Forbes for help with LaTeX.

AMS subject classification: 11P32, 11R09.

$p \mid r''$, $q \mid s'$ and $q \nmid s''$, letting $r = 2r' - r''$ and $s = 2s' - s''$ gives the desired result. ∎

THEOREM 1 (GOLDBACH'S CONJECTURE FOR $\mathbb{Z}[x]$). *Given any polynomial $P(x) \in \mathbb{Z}[x]$, there exist irreducible polynomials $Q(x), R(x) \in \mathbb{Z}[x]$ such that $P(x) = Q(x) + R(x)$.*

PROOF. Note that the theorem is trivially true if $P(x)$ has degree zero. Thus assume $deg(P(x)) \geq 1$. Let $P(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$, $Q(x) = b_n x^n + b_{n-1}x^{n-1} + \cdots + b_0$ and $R(x) = c_n x^n + c_{n-1}x^{n-1} + \cdots + c_0$. We will show that we can choose the b_i's and c_i's to satisfy the theorem. First, choose $b_n, c_n \neq 0$ such that $b_n + c_n = a_n$. Next choose distinct odd primes p and q such that $p \nmid b_n$, $q \nmid c_n$, $p \nmid a_0$ and $q \nmid a_0$. By the Euclidean algorithm, there exist integers k, m satisfying $kp + mq = 1$. Thus for $1 \leq i \leq n-1$, letting $b_i = a_i kp$ and $c_i = a_i mq$ gives $b_i + c_i = a_i$, with $p \mid b_i$ and $q \mid c_i$. Finally, by the above lemma, there exist integers r, s such that $rp + sq = 1$ where $p \nmid r$ and $q \nmid s$. Hence, letting $b_0 = a_0 rp$ and $c_0 = a_0 sq$ gives $b_0 + c_0 = a_0$ with $p \mid b_0$, $q \mid c_0$, $p^2 \nmid b_0$ and $q^2 \nmid c_0$ (since $p, q \nmid a_0$). Since $p \nmid b_n$ and $p \mid b_i$ for all $i \leq n-1$ and $p^2 \nmid b_0$, $Q(x)$ is irreducible by Eisenstein's irreducibility criterion. Similarly, $R(x)$ is irreducible. It is clear by construction that $P(x) = Q(x) + R(x)$, as desired. ∎

There are a few remarks to be made about this proof. The above does not merely prove the existence of $Q(x)$ and $R(x)$, but also gives an algorithm for finding them (given an appropriate choice of p, q). Indeed, the above construction gives an infinite number of pairs $\big(Q(x), R(x)\big)$ that sum to $P(x)$. Given any finite set of such pairs, we can take p and q to be greater than all of the coefficients of the polynomials $Q(x)$ and $R(x)$, giving rise to a pair that is not contained in the given set. One significant difference between this problem and that originally posed by Goldbach is that in allowing negative coefficients, we have not distinguished between a sum and a difference. Perhaps a more natural analogue would require some restriction of 'positivity' all of the polynomials. At first one might think to demand that all coefficients be nonnegative. In this case, we see that $(x^2+1)^2$ cannot be expressed as the sum of two irreducibles; indeed, any polynomial with at least 3 terms, constant term 1, and no degree one term cannot be so expressed. Alternately, if we require that the leading coefficients of all polynomials be positive, then the theorem above remains true. We will now use Eisenstein's Criterion once again to give a proof of the analogue of another unsolved prime number conjecture, namely the problem of whether there exist infinitely many primes of the form $n^2 + 1$.

THEOREM 2. *There exist infinitely many polynomials $p(x) \in \mathbb{Z}[x]$ such that $p(x)^2 + 1$ is irreducible.*

PROOF. Let $p(x) \in \mathbb{Z}[x]$ be any polynomial with all coefficients being even except for the constant and leading terms. Clearly there are infinitely many such

polynomials. Then $p(x)^2$ has all coefficients even except for the constant and leading terms. Let c denote the constant term of $p(x)$. Note that $c^2 \equiv 1 \pmod 4$, since c is odd. Hence 2 divides all non-leading coefficients of $p(x)^2+1$ and divides the constant term, $c^2 + 1$, exactly once. Therefore, by Eisenstein's Criterion, $p(x)^2 + 1$ is irreducible over $\mathbb{Z}[x]$. ∎

It is clear that Eisenstein's Criterion plays an essential role in the proofs of the above results. The analogous problems for natural numbers or for polynomials over finite fields are complicated by the absence of a similar criterion for identifying certain primes. Another reason that these problems are more easily solved for $\mathbb{Z}[x]$ is the high density of irreducibles in $\mathbb{Z}[x]$; indeed, it has been shown that the probability that a randomly chosen polynomial in $\mathbb{Z}[x]$ is irreducible is 1 [Se]. This is not, however, the case for natural numbers or for polynomials over finite fields.

REFERENCES

[EH] G. W. Effinger and D. R. Hayes, *Additive Number Theory of Polynomials Over a Finite Field.* Oxford University Press, 1991.

[Se] J.-P. Serre, *Topics in Galois Theory.* Research Notes in Mathematics **1**. Jones & Bartlett Publishers, 1992.

Department of Mathematics and Statistics
Queen's University
Kingston, Ontario
K7L 3N6
email: 6ar8@qlink.queensu.ca
4cbs1@qlink.queensu.ca

C. R. Math. Rep. Acad. Sci. Canada Vol. **20** (3), 1998 pp. 86–90

ADDITIVE AND SUBTRACTIVE IRREDUCIBLE MONIC DECOMPOSITIONS IN $\mathbb{Z}[X]$

C. BETTS

Presented by M. Ram Murty, FRSC

ABSTRACT. We prove two Goldbach-type theorems for polynomials in $\mathbf{Z}[x]$—the Additive Decomposition Theorem writes a *monic* polynomial as the *sum* of two irreducible monics and the Subtractive Decomposition Theorem writes *any* polynomial as the *difference* of two irreducible monics. The theorems can be used to derive many interesting results, *e.g.* given a monic polynomial P of degree n, we can find appropriate P_i such that $P^n = \sum_{i=0}^{n^2} P_i$, where each P_i is an irreducible monic and $\deg(P_i) = i$.

RÉSUMÉ. Nous démontrons des résultats à propos des analogues de la Conjecture de Goldbach pour l'anneau des polynômes $\mathbf{Z}[x]$. Les résultats les plus importants sont la décomposition d'un polynôme monique comme somme de deux polynômes irréductibles moniques et la décomposition de tout polynôme comme différence de deux polynômes irréductibles moniques. Les théoremes ont beaucoup de conséquences intéressantes, *e.g.*, pour chaque polynôme monique P avec $\deg(P) = n$, il existe des polynômes irréductibles et moniques P_i, satisfaisant $\deg(P_i) = i$, $P^n = \sum_{i=0}^{n^2} P_i$.

1. **Introduction.** The Coleman-Ellis lecture delivered by M. R. Murty at Queen's University in October 1997 discussed some polynomial analogs of the Goldbach conjecture [RIB]. Murty concluded his talk with a challenge/conjecture for the audience: "Can any monic be decomposed as the sum of two irreducible monics?" The following results and investigations arose from the lecture. In particular, Theorem 3 answers Murty's question in the affirmative.

2. **Procedure.** Our proofs[1] are motivated by the Eisenstein Criterion [GAL]:

LEMMA 1. (EISENSTEIN) *If* $f = f_0 + f_1x + \cdots + f_{n-1}x^{n-1} + f_nx^n$ *and there is a prime* p *such that* $p \mid f_i$, $0 \leq i \leq n-1$, $p \nmid f_n$, $p^2 \nmid f_0$, *then* f *is irreducible over* $\mathbb{Q}$ *(and will be referred to as* p-Eisenstein*).*

Recall that a polynomial $f \in R[x]$, R a ring, is *irreducible* if $f = gh$, $g, h \in R[x]$, implies that either g or h is a unit in $R[x]$ [BJN]. Hence if $f \in \mathbb{Z}[x]$ is primitive and

Received by the editors December 1, 1997.
Acknowledgement: M. R. Murty, A. M. Logan and B. J. Betts
AMS subject classification: 11P32, 11R09.
Key words and phrases: additive number theory, algebraic number theory.

[1] Unless otherwise stated, all polynomials will be in $\mathbb{Z}[x]$.

irreducible over $\mathbb{Q}$ then f is irreducible over $\mathbb{Z}$, since 1 and -1 are the only units in $\mathbb{Z}[x]$. We give an illustrative example: $f = 2x^2 + 4 = (2)(x^2 + 2)$ is irreducible over $\mathbb{Q}$, since 2 is a unit in $\mathbb{Q}[x]$, but f is *not* irreducible over $\mathbb{Z}$ [GAL].

With the assistance of the following lemma, we proceed to the statement and proof of the theorems.

LEMMA 2. *Given $z \in \mathbb{Z}$ and distinct primes p, q, then there exist $x, y \in \mathbb{Z}$ such that $x \equiv p \pmod{p^2}$, $y \equiv q \pmod{q^2}$ and $x + y = z$.*

The proof of the lemma is a straightforward application of the Chinese Remainder Theorem, but the proofs of the theorems rely heavily on the result, so we include a proof for completeness.

PROOF. It is clear that p is a particular solution to the congruence $x \equiv p \pmod{p^2}$, hence we can consider the family of solutions given by $\{p + kp^2, k \in \mathbb{Z}\}$. We must choose k and y so that $(p + kp^2) + y = z$ while $y \equiv q \pmod{q^2}$, *i.e.*, $z - (p + kp^2) \equiv q \pmod{q^2}$. Subtracting, we want $-kp^2 \equiv q + p - z \pmod{q^2}$. But p^2 has a multiplicative inverse modulo q^2, say $(p^2)_q^{-1}$, since p^2 and q^2 are coprime. Thus any $k \equiv -(p^2)_q^{-1}(q + p - z) \pmod{q^2}$ will give us an appropriate y. Taking the particular solution $k = -(p^2)_q^{-1}(q + p - z)$, we see that

$$x = p - (p^2)_q^{-1}(p^2)(q + p - z),$$
$$y = z - p + (p^2)_q^{-1}(p^2)(q + p - z),$$

satisfy Lemma 2. ∎

3. The Additive Decomposition Theorem (ADT).

THEOREM 3. (ADT) *If $f \in \mathbb{Z}[x]$ is monic with $\deg(f) = n \geq 1$, then there exist two irreducible monics $P, Q \in \mathbb{Z}[x]$ that will satisfy $\deg(P) = n$, $\deg(Q) = n - 1$ and $P + Q = f$.*

PROOF. Let $f = f_0 + f_1 x + \cdots + f_{n-1}x^{n-1} + x^n$. Our goal is to construct irreducible monics

$$P = P_0 + P_1 x + \cdots + P_{n-2}x^{n-2} + P_{n-1}x^{n-1} + x^n,$$
$$Q = Q_0 + Q_1 x + \cdots + Q_{n-2}x^{n-2} + x^{n-1},$$

such that $P + Q = f$. We have little choice for P_{n-1}; it must be $f_{n-1} - 1$. To make P p-Eisenstein for some prime p, we must have $p \mid f_{n-1} - 1$. Clearly, no such p exists if $f_{n-1} - 1 = \pm 1$. We treat these two cases (in which we cannot apply the Eisenstein Criterion directly) later. For now, assume that $f_{n-1} - 1 \neq \pm 1$ and thus there exists p such that $p \mid f_{n-1} - 1$.

Now choose any other prime q distinct from p. Since p and q are relatively prime, there exist integers m and n such that $mp + nq = 1$. We can proceed with

making P p-Eisenstein and Q q-Eisenstein by setting $P_i = mpf_i$ and $Q_i = nqf_i$, $1 \le i \le n-2$, since $p \mid mpf_i$, $q \mid nqf_i$. Noting that $mpf_i + nqf_i = (mp+nq)f_i = f_i$, we have

$$P + Q = (P_0 + Q_0) + f_1 x + \cdots + f_{n-2}x^{n-2} + f_{n-1}x^{n-1} + x^n.$$

Since P and Q are both monic, no prime divides their leading coefficient. To make P p-Eisenstein, we need $p \mid P_0$ and $p^2 \nmid P_0$. These two conditions are trivially satisfied if $P_0 \equiv p \pmod{p^2}$. Similarly, the corresponding conditions on Q_0 will be satisfied if $Q_0 \equiv q \pmod{q^2}$. We are finished if we can also have $P_0 + Q_0 = f_0$. But Lemma 2 guarantees that such P_0, Q_0 exist. In fact, if we take the particular solutions described in the proof of Lemma 2, setting

$$P_0 = p - (p^2)_q^{-1}(p^2)(q + p - f_0),$$
$$Q_0 = f_0 - p + (p^2)_q^{-1}(p^2)(q + p - f_0),$$

we have completed our construction of P and Q:

$$P = p - (p^2)_q^{-1}(p^2)(q + p - f_0) + mpf_1 x + \cdots + mpf_{n-2}x^{n-2} + (f_{n-1} - 1)x^{n-1} + x^n,$$
$$Q = f_0 - p + (p^2)_q^{-1}(p^2)(q + p - f_0) + nqf_1 x + \cdots + nqf_{n-2}x^{n-2} + x^{n-1}.$$

Since no prime divides 1 (*i.e.*, the leading coefficients of P and Q), we now have that P is p-Eisenstein and Q is q-Eisenstein with $P+Q = f$. By Eisenstein's Criterion, we conclude that P and Q are irreducible over $\mathbb{Q}$. P and Q are monic, hence primitive, and therefore irreducible over $\mathbb{Z}$ as well.

Now we deal with the first special case, namely when $f_{n-1} = 2$. Consider $f^*(x) = f(x+1)$. f^* is clearly monic, has $\deg(f^*) = n$, and has coefficient value $f^*_{n-1} = n + 2$. Our original assumption that $\deg(f) = n \ge 1$ implies $f^*_{n-1} - 1 = n + 2 - 1 > 1$. Thus it follows from our previous work that we can write f^* as the sum of two irreducible monics, say P^* and Q^*. Reversing the translation, set $P(x) = P^*(x-1)$, $Q(x) = Q^*(x-1)$. The polynomials P and Q are obviously still monic and irreducible (translation has no effect on irreducibility). Thus

$$f(x) = f^*(x-1) = P^*(x-1) + Q^*(x-1) = P(x) + Q(x)$$

and we have succeeded in writing f as the sum of two irreducible monics. When $f_{n-1} = 0$, consider the translation $f^*(x) = f(x-1)$ and make similar observations. ∎

ADT has many interesting consequences, one of which we describe in the following corollary.

COROLLARY 4. *Given a monic* $P \in \mathbb{Z}[x]$ *with* $\deg(P) = n$ *and an integer* k, $0 \le k \le n-1$, *then there exists a sequence* $\{P_i\}_{i=k}^n$, *with each* $P_i \in \mathbb{Z}[x]$ *an irreducible monic and* $\deg(P_i) = i$, *such that* $\sum_{i=k}^n P_i = P$.

PROOF. By ADT, we can decompose P into two irreducible monics P_n, Q_{n-1} with $\deg(P_n) = n$, $\deg(Q_{n-1}) = n-1$ such that $P_n + Q_{n-1} = P$. Again by ADT, decompose Q_{n-1} into P_{n-1}, Q_{n-2} and so on by induction until we have $Q_{k+1} = P_{k+1} + Q_k$. Set $P_k = Q_k$. Then $P = \sum_{i=k}^{n} P_i$ and $\deg(P_i) = i$. ∎

We single out an aesthetically pleasing special case of Corollary 4 in the following remark:

REMARK 5. *If $P \in \mathbb{Z}[x]$ is monic with $deg(P) = n$, then we can find irreducible monics $P_i \in \mathbb{Z}[x]$ that will satisfy* $\deg(P_i) = i$ *and* $P = P_0 + P_1 + \cdots + P_{n-1} + P_n$.

There is of course an endless variety of such decomposition formulas, particularly when ADT is combined with the Subtractive Decomposition Theorem. We conclude this section by observing that $P^{\deg(P)}$ is monic if P is monic and has degree $(\deg(P))^2$. The result outlined in the abstract is now immediate from Remark 5.

4. The Subtractive Decomposition Theorem (SDT)

THEOREM 6. (SDT) *If $f \in \mathbb{Z}[x]$, then there exist two irreducible monics $P, Q \in \mathbb{Z}[x]$ such that $P - Q = f$.*

PROOF. Let $f = f_0 + f_1 x + \cdots + f_{n-1}x^{n-1} + f_n x^n$. Again motivated by the Eisenstein Criterion we construct

$$P = P_0 + P_1 x + \cdots + P_{n-1}x^{n-1} + P_n x^n + x^{n+1},$$
$$Q = Q_0 + Q_1 x + \cdots + Q_{n-1}x^{n-1} + Q_n x^n + x^{n+1}.$$

Select two distinct primes p and q and pick m and n so that $mp + nq = 1$. Set $P_i = mpf_i$ and $Q_i = -nqf_i$, $1 \le i \le n$. Select P_0 and Q_0 according to the procedure outlined in Theorem 3. Then P is p-Eisenstein and Q is q-Eisenstein and $P - Q = f$. Both polynomials are monic and hence irreducible over $\mathbb{Z}$. ∎

SDT admits many results of similar flavor to Corollary 4. In particular, we observe the following:

COROLLARY 7. *If $P \in \mathbb{Z}[x]$ with* $\deg(P) = n$, *then there are sequences $\{P_i\}_{i=k}^{n+1}$, $\{Q_i\}_{i=k}^{n+1}$, $0 \le k \le n$, each $P_i, Q_i \in \mathbb{Z}[x]$ an irreducible monic with* $\deg(P_i) = \deg(Q_i) = i$, *such that $\sum_{i=k}^{n+1} P_i - Q_i = P$.*

PROOF. Use SDT to get P_{n+1}, Q_{n+1} and then apply Corollary 4 to each. ∎

COROLLARY 8. *If $f \in \mathbb{Z}[x]$, then there exist irreducible polynomials $P, Q \in \mathbb{Z}[x]$ such that $P + Q = f$.*

PROOF. Choose P and Q' by Theorem 6 such that $P - Q' = f$. Set $Q = -Q'$. -1 is a unit in $\mathbb{Z}[x]$, so Q is irreducible, and we have the result: $P + Q = P - (-Q) = P - Q' = f$. ∎

5. **Concluding Remarks.** The preceding results clearly demonstrate the power of having an irreducibility test (even a partial test like Eisenstein) for a ring/field. The difficulty of the Goldbach Conjecture for the integers or polynomials over a finite field is largely due to the lack of an appropriate primality test in these settings.

Furthermore, as the referee explained, the probability of a randomly selected polynomial in $\mathbb{Z}[x]$ being irreducible is 1. Again, this is not the case with prime integers or irreducible polynomials over a finite field. The lower density of the irreducibles does not exhibit an obvious route to solving the Goldbach Conjecture over an arbitrary ring.

Finally, the referee pointed out that there is a paper by D. Hayes, "A Goldbach Theorem for Polynomials with Integral Coefficients", American Mathematical Monthly, Volume 72, No. 1 (1965), pp. 45–46, that discusses an additive decomposition by irreducible polynomials as in Corollary 8. Also, the referee raised some issues about density of irreducibles and number of representations, which will be the subject of a forthcoming paper.

References

[GAL] J. A. Gallian, *Contemporary Abstract Algebra.* Third Edition, D. C. Heath and Company, Toronto, 1994, Ch. 17.

[BJN] P. B. Bhattacharya, S. K. Jain and S. R. Nagpaul, *Basic Abstract Algebra.* Cambridge University Press, New York, 1995.

[RIB] P. Ribenboim, *The New Book of Prime Number Records.* Springer-Verlag, New York, 1996, 291.

[NAT] M. Nathanson, *Additive Number Theory.* Springer-Verlag, New York, 1996.

Department of Mathematics and Statistics
Queen's University
Kingston, ON
K7L 3N6
email: 3ceb8@qlink.queensu.ca

C. R. Math. Rep. Acad. Sci. Canada Vol. **20** (3), 1998 pp. 91–96

CONCURRENT CATASTROPHES: THE SUM OF TWO INDEPENDENT GUMBELS

R. B. LEIPNIK

Presented by G. F. D. Duff, FRSC

RÉSUMÉ. Les lois de probabilité des sommes des variables aléatoires indépendantes du type Gumbel ayant des paramètres a_1, b_1; a_2, b_2 ont été calculeés comme séries exponentielles avec des coefficients factoriels et cosécantes. Au cas où le quotient de paramètres b_1 et b_2 est un nombre irrationnel (c'est-à-dire le cas ≪non-mesurable≫) on arrive à un résultat différent de celui où le quotient n'est pas irrationnel (c'est-à-dire le cas ≪mesurable≫). Le résultat de la somme d'une variable aléatoire Gumbel ≪maximum≫ et une variable Gumbel ≪minimum≫ est une loi de probabilité logistique générale. La somme de deux variable aléatoires du type Gumbel ≪maximum≫ donne un ensemble de fonctions Basset et des exponentielles. Le méthode de calcul utilise l'intégrale complexe de Cauchy. La convergence mathématique des lois de probabilité fut établie au cas où le quotient $\beta = b_1/b_2$ est un nombre irrationel algébraique ou quasi-transcendantal en utilisant le théoreme du Liouville. Au cas où le quotient β est mesurable, les lois des probabilité ainsi obtenues dépendent de la structure arithmétique du β. Des applications aux innondations simultanées sont citées.

1. **Background.** E. J. Gumbel worked on extreme value problems, arriving in 1934 at the famous Gumbel distributions [2] (see Galambos [1]). Applications are to wave heights, river floods, rainfall, strength of materials, stock markets, breakdown voltages, and miscellaneous catastrophes. The sum of two or more independent Gumbels indicates the combined effects of extreme events. The total flux below the confluence of two rivers, flooded by independent storms is a motivating example. Simulation by convolution sums is expensive for long-tailed distributions, for one set of parameters, and quite impractical for many. Conventional asymptotic theory is inapplicable; closed forms are the last resort.

These are not available in the literature. The Gumbel case is easier than the lognormal case (Leipnik [3]); the techniques of classical analysis and number theory used in [3] are effective here. A decent theory of sums of extreme variables is difficult; this exploratory paper shows what to expect in general.

Received by the editors December 8, 1997.
AMS subject classification: 60.

2. **Gumbel maximum and minimum distributions.** The Gumbel "maximum" c.d., for a variable of location a and scale b is

$$G_{a,b}(x) = e^{-y}, \quad y = e^{-(x-a)/b}, \quad b > 0 \tag{1}$$

with density $g_{a,b}(x) = ye^{-y}/b$. The c.f. is, for real u,

$$\phi_{a,b}(u) = \int_{-\infty}^{\infty} e^{iux}\, dG_{a,b}(x) = \int_0^{\infty} e^{iua} y^{-iub} e^{-y} (y/b)\, dx = e^{iua}\Gamma(1 - ibu), \text{ so} \tag{2}$$

$$\phi_{a,b}(u) = e^{iua} \frac{\pi iub}{\sin(\pi iub)} \frac{1}{\Gamma(1 + iub)} \tag{3}$$

which extends to the z-plane, with imaginary poles.

Let $X_{a_1,b}$ denote a Gumbel "maximum" random variable with location a_1 and scale b, and let $X^-_{a_2,b}$ denote a Gumbel "minimum" random variable; so $G^-_{a_2,b}(x) = 1 - G_{a_2,b}(2a_2 - x)$, density $g^-_{a_2,b}(x) = g_{a_2,b}(2a_2 - x)$. The c.f.'s of $X^-_{a_2,b}$ and $-X_{a_1,b}$ are

$$\phi^-_{a_2,b}(u) = e^{ia_2u}\Gamma(1 + ibu), \quad \tilde{\phi}_{a_1,b}(u) = e^{-ia_1u}\Gamma(1 + ibu) \tag{4}$$

3. **Sum of maximum and minimum Gumbels of equal scale.** Clearly $L = X^{(1)}_{a_1,b} + X^{(2)^-}_{a_2,b}$ with independent X's has c.f.

$$\psi(u) = e^{iau}\Gamma(1 + ibu)\Gamma(1 - ibu) = e^{iau} \cdot \frac{\pi ibu}{\sin(\pi ibu)}, \quad a = a_1 + a_2 \tag{5}$$

The poles of $e^{-ixz}\phi_{a,b}(z)$ are simple and located at $z_n = -in/b$, $n = 1, 2, \ldots$, the upper poles of $e^{-izx}\psi(z)$ are at $z_p^+ = ip/b$, $p = 1, 2, \ldots$. The residue series converges for $a - x > 0$, so the density $h^-(x)$ of L for $x < a$ is by (5) and a little algebra

$$h^-(x) = \sum_{p=1}^{\infty} pe^{-p(a-x)/b}(-1)^{p-1}/b = e^{-(a-x)/b}\big([1 + e^{-(a-x)/b}]^2 b\big)^{-1} \tag{6}$$

As to the density $h^+(x)$ for $x > a$, the lower poles of $e^{-ixz}\psi(z)$ are at $z_p = -ip/b$. So, as above,

$$h^+(x) = e^{-(x-a)/b}\big([1 + e^{-(x-a)/b}]^2 b\big)^{-1}, \quad h(a) = \frac{1}{2}\big(h^+(a) + h^-(a)\big) = (4b)^{-1} \tag{7}$$

Thus (6) and (7) yield for the density and c.d. of L

$$h(x) = e^{-|x-a|/b}\big([1 + e^{-|x-a|/b}]^2 b\big)^{-1}, \quad a = a_1 + a_2; \quad H(x) = [1 + e^{-(x-a)/b}]^{-1} \tag{8}$$

A similar result holds for $D = X^{(1)}_{a_1,b} - X^{(2)^-}_{a_2,b}$, except that now a is $a_1 - a_2$.

This distribution (8) is called logistic, and is used to fit income distributions, though its density is symmetric about $x = a$. Its c.f. (5) has long been known, of course. The Gumbel connection is known to this extent only.

4. **Sum of Two Independent Gumbels of Same Type, Scale Ratio Incommensurable.** Given two independent Gumbels of maximum type with parameters a_1, b_1 and a_2, b_2, the characteristic function of the sum variable $Y_2 = X^{(1)}_{a_1,b_1} + X^{(2)}_{a_2,b_2}$ is

(9)
$$\phi_2(u) = \left(\frac{e^{iau}}{\Gamma(1+ib_1u)\Gamma(1+ib_2u)}\right)\frac{(\pi ib_1u)(\pi ib_2u)}{\sin(\pi ib_1u)\sin(\pi ib_2u)}, \quad a = a_1 + a_2,\ u \text{ real.}$$

The first factor has no poles in the lower half plane. The second factor has (if b_1 and b_2 are incommensurable) two distinct sets of simple poles, $z^{(1)}_m = -\frac{im}{b_1}$, $z^{(2)}_n = -\frac{in}{b_2}$ for $m, n = 1, 2, \ldots$. The problem is to calculate the density $h_2(x)$ and c.d. $H_2(x)$ of Y_2.

Utilizing a sequence of semi-circles S_n in the lower half-plane, the Cauchy formula for $h_2(x)$ is obtained in terms of the two sets of residues as

(10)
$$h_2(x) = \pi b_1 b_2 \sum_{n=1}^{\infty} \frac{n^2(-1)^{n-1}}{n!}\left[\frac{e^{-nx'/b_1}\csc(n\pi b_2/b_1)}{b_1^3\Gamma(1+nb_2/b_1)} + \frac{e^{-nx'/b_2}\csc(n\pi b_1/b_2)}{b_2^3\Gamma(1+nb_1/b_2)}\right],$$

$$x' = x - a_1 - a_2.$$

The signs alternate due to $(-1)^{n-1}$ and cosecants.

The cumulative distribution H_2 of Y_2 can be obtained by integrating termwise over $[x, \infty)$.

Series (10) converges for all irrational-algebraic scale ratios $\beta = b_2/b_1$ and for many transcendental β, as shown in the Appendix. Results where both Gumbel variables are of "minimum" type may be obtained by replacement of b_1, b_2 by $-b_1$, $-b_2$. The case of commensurable scales is deferred to Section 6.

5. **Sum of Two Gumbels of Opposite Type, Different Scales.** When one Gumbel is of "maximum," the other of "minimum" type, but of different scales, the results resemble the logistic. If $L = X^{(1)}_{a_1,b_1} + X^{(2)-}_{a_2,b_2}$, which may be called the dual case, and $b_2 < b_1$, then the c.f.

$$\psi(z) = e^{iaz}\frac{\pi ib_1z}{\sin(\pi ib_1z)}\frac{\Gamma(1+ib_2z)}{\Gamma(1+ib_1z)}, \quad a = a_1 + a_2, \tag{11}$$

whose poles in the lower-half plane are at $z_n = -in/b_1$. Thus by residues

$$h_2(x) = \sum_{n=1}^{\infty}\frac{(-1)^{n-1}e^{n(a-x)/b_1}\Gamma(1+nb_2/b_1)}{b_1(n-1)!}, \tag{12}$$

a generalized logistic. Convergence for all x is implied by

$$\left|\frac{\Gamma(1+nb_2/b_1)}{(n-1)!}\right| = 0(n^{(b_2/b_1)-1}),$$

and $H_2(x)$ results from termwise integration over $[x, \infty)$.

However, if $b_2 > b_1$, write

$$\psi(z) = e^{iaz} \frac{(\pi i b_2 z)}{\sin(\pi i b_2 z)} \frac{\Gamma(1 - i b_1 z)}{\Gamma(1 - i b_2 z)} \tag{13}$$

By a repetition of the derivation of (12), the density is found to be

$$h_2(x) = \sum_{n=1}^{\infty} \frac{(-1)^{n-1} e^{n(x-a)/b_2} \Gamma(1 + n b_1/b_2)}{b_2 (n-1)!} \tag{14}$$

6. Commensurable Cases for the Sum of Two Independent Gumbels of the Same Type. If the parameters b_1 and $b_2 \geq b_1$, are commensurable, and $\frac{b_2}{b_1} = \frac{b_2^*}{b_1^*}$ in lowest integral terms, with $b_2 = b_2^* b$, $b_1 = b_1^* b$, there are really two cases for the sum of two independent "maximum" Gumbels. In case I, equal scales, $b_1^* = b_2^* = 1$, so that $z_n^{(1)} = -in/b_1 = -in/b = -in/b_2 = z_n^{(2)}$ and all the poles are double. In case II, $b_2^* > 1$, so that only a fraction of the poles are double. It is easy to check that the set D of double poles is obtained with $n_1 b_1^* = n_2 b_2^* = n$, while the two sets of simple poles are the "interrupted" sets,

$$P^{(j)} - D = \{z_1^{(j)}, \ldots z_{b_j^*-1}^{(j)}; z_{b_j^*+1}^{(j)}, \ldots z_{2b_j^*-1}^{(j)}; \ldots\} = \{z_n^{(j)'}\}, \quad j = 1, 2 \tag{15}$$

If $b_1^* = 1$, then $P^{(1)} - D$ is the empty set. From (15), we see

$$z_\nu^{(j)'} = z_{\tau_j(\nu)}^{(j)}, \text{ where } \tau_j(\nu) = \nu + \left[(\nu - 1)/(b_j^* - 1)\right], \quad \nu = 1, 2, \ldots; j = 1, 2, \tag{16}$$

and $[\cdot]$ is the greatest integer function. These just skip multiples of b_j^*. The partial simple pole contributions yield

$$h_2^{(1)}(x) = \pi b_1 b_2 \sum_{\nu=1}^{\infty} \frac{\tau_1^2(\nu)(-1)^{\tau_1(\nu)-1}}{(\tau_1(\nu))!} \left[\frac{e^{-\tau_1(\nu)x'/b_1} \csc(\tau_1(\nu)\pi b_2/b_1)}{b_1^3 \Gamma(1 + \tau_1(\nu) b_2/b_1)} \right] \tag{17}$$

from the poles in $P^{(j)} - D$. Then $h_2^{(2)}(x)$ is obtained by $\tau_1 \to \tau_2$, $b_1 \to b_2$, $b_2 \to b_1$ in (17).

Since b_2^* and $\nu + \left[\frac{\nu - 1}{b_1^* - 1}\right]$ are not divisible by b_1^*, in case II, $\tau_1(\nu) b_2/b_1 = \tau_1(\nu) b_2^*/b_1^*$ is not an integer. Similarly, $\tau_2(\nu) b_1^*/b_2^*$ is not an integer, and so the cosecant values entering $h_2^{(1)}(x)$ and $h_2^{(2)}(x)$ are finite. Since $\nu \to \infty$ implies $\tau(\nu) \to \infty$, convergence of (17) follows from the Appendix.

The double-pole contributions are more tedious. Each of these arises from a residue involving the first derivative of a product of seven different terms, and so the resulting expression has seven additive terms of seven multiplicative terms.

Now let

$$P_\nu(z) = \frac{z^2 e^{-izx'}(z - z_\nu)^2}{Q(z)}, \quad Q(z) = \prod_{k=1}^{2} (\sin \pi i b_k z) \Gamma(1 + i z b_k) \tag{18}$$

and let temporarily $z_\nu = -i\nu/b$ be the locations of the double poles, for $\nu = 1, 2, \ldots$. A detailed study of $dP_\nu/dz = \sum_{j=1}^{7} T_{j\nu}(z)$, reveals that $(T_{j\nu}/P_\nu)$ is the vector

$$\left(\frac{2}{z}, -ix', \frac{2}{z - z_\nu}, \lambda_1(z), \lambda_2(z), \mu_1(z), \mu_2(z)\right) \tag{19}$$

where $\lambda_j(z) = -\pi i b_j \cot(\pi i b_j z)$, $\mu_j(z) = -ib_j\psi(1 + ib_j z)$, and $\psi(z) = \Gamma'(z)/\Gamma(z)$ is now Euler's function. The classic cotangent series

$$\frac{1}{w} - \pi i b \cot(\pi i b w) = 2b^2 w \sum_{p=1}^{\infty} \frac{1}{w^2 - p^2}$$

yields eventually the double-pole contribution as a new Basset-type function

$$h_2^{(3)}(x) = \sum_{\nu=1}^{\infty} \frac{\nu^2 e^{-\nu x'/b}(-1)^{\nu(b_1^* + b_2^*)}}{b^2(\nu b_1^*)!(\nu b_2^*)!} \cdot \left[x' + b_1\psi(1 + \nu b_1^*) + b_2\psi(1 + \nu b_2^*) - \frac{2b}{\nu}\right] \tag{20}$$

The series (20) converges with Bessel speed for large ν. This result displays a kind of chaos with respect to commensurable b_1 and b_2.

The total density is

$$h_2(x) = h_2^{(1)}(x) + h_2^{(2)}(x) + h_2^{(3)}(x), \tag{21}$$

from (17) and (20). In case I, $b_1^* = b_2^* = 1$, $h_2^{(1)}(x) = h_2^{(2)}(x) = 0$, and so $h_2(x)$ reduces after some algebra to $\dfrac{2e^{-x'/b}}{b} K_0(2e^{-x'/2b})$ where $K_0(y)$ is a Basset function (Watson [4]).

7. **Concurrent Catastrophes.** Catastrophes are rare events. Concurrent ones, rarer still, are seldom available for analysis. Separated storms in adjacent terrene watersheds can cause flood stages in many streams and rivers, which are more devastating near to and below their confluences. In structural mechanics, an extreme stress from temporary overuse may be coincident with an extreme stress from wind or snowfall, *etc.* Two weather systems in close succession may arrive from the pole and the equator in temperate latitudes, resulting in squalls, tornadoes, *etc.* If a Gumbel distribution is a reasonable model for a flux-type variable, then a sum of Gumbels fits a multi-flux scenario. The cost of concurrent catastrophes merits study.

Professor H. Loaiciga of UCSB intends to apply the Gumbel sum model to some river flow and cumulative rainfall data. The writer wishes to acknowledge the encouragement of Professor Loaiciga and the help of Mr. Troy Reid, a research assistant at UCSB, in checking the tedious calculations.

8. **Appendix. Convergence of cosecant series.** The cosecant series obtained formally in Sections 4, 6 can be shown to converge rapidly by making several estimates, some rather elementary, and another using a famous result of Liouville in approximation of algebraic numbers by sequences of rationals, or stronger modern theorems, by A. Baker, *etc.*

The series (15) involves two parts of the essential form

$$\sum_n \frac{n^2 z^n \csc(n\pi\beta)}{n!\,\Gamma(1+n\beta)} = \sum_n \frac{n^2 z^n \Gamma(1-n\beta)}{n!}, \quad \beta \text{ irrational.}$$

A long elementary argument shows that if $n^{\delta n}[(n\beta) \mod 1][1-(n\beta) \mod 1] = n^{\delta n} t(n\beta) \to \infty$ as $n \to \infty$ for each $\delta > 0$ then the series converges for all z. An application of Liouville's theorem shows that if β is an algebraic number of degree g, then $t(n\beta) \geq \frac{K^2}{(n^2)^{g+\epsilon-1}}$ for each $\epsilon > 0$ and some $K = K(\epsilon)$, so $n^{\delta n} t(n\beta) \to \infty$. The result $n^{\delta n} t(n\beta) \to \infty$ also holds for mildly transcendental β.

For the commensurable case, where $\beta = b_1/b_2 = b_1^*/b_2^*$ in lowest terms, the skipping sequence $\tau(n) = n + [(n-1)/(b_2^* - 1)]$ provides values $\langle \tau(n)\beta \rangle = (\tau(n)\beta) \mod 1$ which take on only the values $1/b_2^*, \ldots (b_2^* - 1)/b_2^*$ in some order. Thus $t(\tau(n)\beta)$ takes values bounded below by $(b_2^* - 1)/b_2^{*2})$ so that $n^{\delta n} t(\tau(n)\beta) \to \infty$ trivially for every $\delta > 0$, as $n \to \infty$. This proves the convergence of the "skipping" cosecant series.

References

1. J. Galambos, *The Asymptotic Theory of Extreme Order Statistics.* Wiley, New York, 1978.
2. E. J. Gumbel, *Les moments des distributions finales de la première et de la dernière valeur.* C. R. Acad. Sci. Paris **198**(1934), 141–143.
3. R. B. Leipnik, *On lognormal random variables.* J. Austral. Math. Soc. Ser. A **32**(1991), 327–347.
4. G. N. Watson, *Theory of Bessel Functions.* 2nd ed. (reprinted), Cambridge University Press, 1952.

Department of Mathematics
University of California
Santa Barbara, CA 93106
USA
email: leipnik@math.ucsb.edu