ACTA ARITHMETICA
105.3 (2002)

Partitions in the prime number maze

by

Michael I. Hartley (Klang)

1. Introduction. Paulsen ([6]) defined the "prime number maze" G_1 as follows. G_1 is a directed graph, whose vertices are the prime numbers. There is an edge in G_1 from p to q if and only if their binary representations have Hamming distance 1, and if $3p \geq q$. That is, if and only if the binary representations of p and q differ by exactly one digit, and that digit may only be the first digit of q if we are merely prepending a single digit (1) to p. For example, there would be bidirectional edges between $61 = 111101_2$ and $53 = 110101_2$, and between $13 = 1101_2$ and $29 = 11101_2$. However, although there would be an edge from $37 = 100101_2$ to $5 = 101_2$, there is none from 5 back to 37. Nonetheless, there is a path from 5 to 37, as pointed out in [6], as follows: $5 \to 13 \to 29 \to 61 \to 53 \to 37$.

The structure of the prime number maze appears to be quite intricate. Paulsen discovered ([6]) that the shortest path in this maze from 2 to 353 leads through primes exceeding 132 digits, then suddenly dropping through $2^{441} + 2^{392} + 2^{27} + 353 \to 2^{392} + 2^{27} + 353 \to 2^{27} + 353 \to 353$. In fact, there is a tiny chance that the shortest path to this number must go even higher, since Paulsen used Miller–Rabin strong pseudoprimality tests, rather than strict primality tests, on the larger numbers in the sequence.

Furthermore, Paulsen noted that $G_1' = G_1 - \{3\}$ is divided into at least two "partitions". Let G_p be the subgraph of G_1 induced by the subset of all the vertices q of G_1 for which there is a path from p to q. Similarly define G_p'. It turns out that if $11 \in G_p'$, then G_p' and G_2' are disjoint, as may be proven using a simple argument involving what Paulsen calls the "parity" of a prime number.

Let $p > 3$ be prime. We say p has *correct parity* if either $p \equiv 2 \bmod 3$ and p has an even number of 1 bits in its binary representation, or $p \equiv 1 \bmod 3$ and p has an odd number of 1 bits in its binary representation. Otherwise, it has *incorrect parity.* Paulsen proved (Proposition 1 of [6]) that any edge in G_1 between $p, q > 3$ must preserve parity. He uses this fact to show that

2000 *Mathematics Subject Classification*: 11A41, 11B05, 11R18.

G_1' consists of at least two partitions, the α-partition, containing 5, and the β-partition, containing 11. Note that G_2 contains the α-partition. All the primes in the α-partition have correct parity, all those in the β-partition have incorrect parity.

There are other partitions as well, in fact from Proposition 3 of [6] we know that G_1 has infinitely many isolated points. The α- and β-partitions are of interest because they appear to be infinite.

In fact, Paulsen conjectured that there are more infinite partitions than just the α- and β-partitions. He noted the apparent existence of what he called the γ- and δ-partitions of G_1'. Their main features are characterized in Table 1, which is also found in [6].

Table 1. The partitions as conjectured by Paulsen

	Lowest prime	Starting point	Comments
α-partition	2	2	"main maze"
β-partition	11	547	can reach α via 3
γ-partition	277	4957	incorrect parity
δ-partition	683	35759	correct parity

Paulsen left it as an unsolved problem whether or not these are the only infinite partitions, and whether or not the γ- and β-, or the α- and δ-partitions eventually join up. Evidently, from parity arguments, the γ-partition cannot join up with α or δ, nor δ with β, except possibly through the number 3.

Later in this article, these unanswered questions will be settled, and we will see a more satisfactory way to delineate the partitions.

2. The base b mazes. In order that the results may be stronger, we first of all define the base b maze G_*^b as follows.

$G = G_*^b$ is a graph whose vertices are the primes, such that there is an edge from p to q in G if and only if their base b representations $p = e_0b^0 + e_1b^1 + \ldots + e_mb^m$ and $q = f_0b^0 + f_1b^1 + \ldots + f_nb^n$ $(0 \leq e_i, f_i < b$, $e_m, f_n \neq 0)$ are such that either $n = m$ and (for some k) $e_i = f_i$ for all $i \neq k$ and $|e_k - f_k| = 1$, or $n = m + 1$, $f_n = 1$, and $e_i = f_i$ for $0 \leq i \leq m$.

Some examples are in order. Choosing, for familiarity's sake, $b = 10$, we find that there are edges between 2 and 3, and also between 3 and 13, and between 13 and 23, 13 and 113, and 113 and 103. However, although an edge exists from 103 back to 3, this last edge is unidirectional. We cannot go from 3 directly to 103.

An exploration of G_*^{10} turns out to be less interesting than that of the original prime number maze. The graph seems to have many small disconnected components. Defining the *generated subgraph* G_p^b to be the subgraph of G_*^b containing all vertices q for which a path exists from p to q, one finds that $G_2^{10} = \{2, 3, 13, 23, 103, 113, 1103\}$, $G_5^{10} = \{5\}$, $G_7^{10} = \{7, 17\}$, $G_{11}^{10} = \{11\}$, and so on. The situation seems to improve only slightly as p increases. The largest G_p for any p less than 2 million is G_{262331}, which has 34 elements, the smallest and largest of which are 262231 and 1111100262101.

A heuristic argument from [6] suggests one reason why this should be the case. Given a large prime N, there are of order $2((b-1)/b)\log_b N$ numbers which differ from N according to the rules of the maze. A fraction of order $1/\ln N$ of these should be prime, on average. It follows that there are of order $2((b-1)/b)\ln b$ edges leading out from N, on average. This will be less than 1 for all bases $b > 4$, hence we may make the following conjecture.

2.1. Conjecture. *For no prime p or base $b > 2$ is the subgraph G_p^b of the base b maze infinite.*

Reason. For $b > 4$, the above heuristic argument shows that the average valence of a vertex should be less than one, making the connected components finite. For $b = 4$ and $b = 3$, the argument gives average valences greater than 1, but these expected average valences are sufficiently reduced by the following results to make the conjecture reasonable. ■

An exploration of the base b mazes for various b reveals that the heuristics are not sufficient to explain the sizes of the components discovered. To shed more light on this matter, we must turn to the next theorem.

First, define the *digit sum* of $p \in G_*^b$ to be $\delta_1^b(p) = e_0 + e_1 + \ldots + e_m$, where $p = e_0 b^0 + e_1 b^1 + \ldots + e_m b^m$ is the base b representation of p.

Note that if there is an edge of G_*^b between p and q, then $\delta_1^b(p) = \delta_1^b(q) \pm 1$. Note also that if r is any divisor of $b-1$, then $r \mid p$ if and only if $r \mid \delta_1^b(p)$. This leads immediately to the following:

2.2. Theorem. *If $b > 2$, the graph G_*^b has infinitely many disjoint components.*

Proof. Let P be the set of primes dividing $b-1$, and let $N = \{\delta_1^b(p) : p \in P\}$. A path in $G_*^b - P$ maps to a path in the graph Z whose vertices are the positive integers, and for which there is an edge between n and m if $|n-m| = 1$ and $\mathrm{GCD}(n, b-1) = 1$ or $n \in N$, and $\mathrm{GCD}(m, b-1) = 1$ or $m \in N$. Since (if $b > 2$) the graph Z has infinitely many disjoint components, so does G_*^b. ■

In fact, for odd b, the graph Z used in the above proof consists mostly of isolated vertices, which means the same is true of G_*^b. This stands to reason, since if p and q satisfy the conditions for them to share an edge, and if b is odd, then one of p or q must be even. In this case, the most interesting generated subgraphs would contain at most four vertices: $G^b_p = \{p, 2, 3, b+2\}$, if $b+2$ is prime, and $p = b^n + 2$ (for some n) is also prime.

For $b = 4$ (and $b = 10$), the digit sum is forbidden (in general) to be a multiple of 3. This is also quite restrictive, since it forces us to alternately add 1 and subtract 1 from digits of the numbers we meet as we walk through the maze.

For $b = 2$, the digit sum tells us nothing at all about the primality of the number. There appear to be primes with every possible digit sum (except 1).

3. Alternating digit sums. Define the *alternating digit sum* $\delta^b_{-1}(p)$ of p by $\delta^b_{-1}(p) = e_0 - e_1 + e_2 - \ldots + (-1)^m e_m$, where $p = e_0 b^0 + e_1 b^1 + \ldots + e_m b^m$ is the base b representation of b.

As with the digit sums, we can use alternating digit sums to prove a result about the structure of G^b_*. In this case, we use the fact that for any factor r of $b+1$, r divides p if and only if r divides $\delta^b_{-1}(p)$. This yields a theorem exactly like Theorem 2.2, except that it also applies when $b = 2$.

3.1. Theorem. *If $b > 1$, the graph G^b_* has infinitely many disjoint components.*

Proof. The proof is almost identical to that of Theorem 2.2, but uses δ^b_{-1} and $b+1$ instead of δ^b_1 and $b-1$. ∎

This result, along with Theorem 2.2 and the heuristics which precede it, suggest that the mazes with the largest components will be those base b mazes for which b is not large, and neither of $b \pm 1$ have small prime factors. Indeed, the base 12 maze has many large components. The smallest p for which $|G^{12}_p| > 100$ is only $p = 6907_{10} = 3\mathrm{BB}7_{12}$. The elements of G^{12}_{6907}, numbering 122 in all, range from $991_{10} = 6\mathrm{A}7_{12}$ to $5593001719_{10} = 1101102987_{12}$. G^{12}_{58453} has 154 elements.

For the original prime number maze, with $b = 2$, Theorem 3.1 allows us to make the following definitions. Let the k-partition Γ_k of $G_1 = G^2_*$ be the set of all primes p such that $\delta^2_{-1}(p)$ equals $3k+1$ or $3k+2$.

3.2. Theorem. *Let $p \in \Gamma_i$ and $q \in \Gamma_j$. If there is a path in G_1 from p to q, then either $i = j$, or $\{i, j\} = \{-1, 0\}$ and the path contains the number 3.*

Proof. When $b = 2$, the alternating digit sum $\delta^2_{-1}(p)$ is a multiple of 3 if and only if p is a multiple of 3. Therefore, if $p' \in \Gamma_i$, and there is an edge in G_1 between p' and q', then either $q' = 3$, or $q' \in \Gamma_i$ also. Therefore, it is impossible for a path from $p \in \Gamma_i$ to leave Γ_i except via 3. The fact that 3 is only reachable from Γ_{-1} and Γ_0 completes the proof. ∎

Note that the α-, β-, γ- and δ-partitions as defined in [6] more or less correspond to Γ_0, Γ_{-1}, Γ_1 and Γ_{-2} respectively. However, [6] places 2 in the

α-partition, but the fact that $\delta^2_{-1}(2) = -1 = 3(-1) + 2$ places it in Γ_{-1}. The prime 2 is anomalous in this respect, in that the only edge from or to 2 passes directly through 3, and the only edges out of 3 lead to 2 or into Γ_0, so that $G_2 - \{2, 3\} \subset \Gamma_0$.

Note also that the partitions Γ_k cover all primes except 3, whereas the partitions of [6] exclude isolated primes, and other finite subgraphs of G_1 (if any exist).

Paulsen was unable to discover to which of his partitions (β- or γ-) the prime 6379 belongs. Using the fact that $6379 = 1100011101011_2$, we can deduce that if it is in either, it must be in the β-partition, since $\delta^2_{-1}(6379) = -2$.

The partitions Γ_k are strongly linked to the concept of parity.

3.3. Theorem. *A prime $p > 3$ has correct parity if and only if it is in Γ_k for some even k.*

Proof. Note that $\delta^2_1(p)$ and $\delta^2_{-1}(p)$ are either both even or both odd. If p has correct parity, then if $\delta^2_1(p)$ is even, so is $\delta^2_{-1}(p) = 3k + 2$, and if $\delta^2_1(p)$ is odd, so is $3k + 1$. Either way, k must be even. Conversely, if p has incorrect parity, k must be odd. ■

Table 2. The partitions Γ_k

Γ_k	Minimum prime	Starting point
Γ_0	5	5
Γ_{-1}	2	547
Γ_1	277	4,957
Γ_{-2}	683	35,759
Γ_2	17,749	82,261
Γ_{-3}	43,691	2,271,403
Γ_3	1,398,037	55,923,157
Γ_{-4}	2,796,203	145,402,811
Γ_4	72,701,269	3,310,702,933
Γ_{-5}	715,827,881	28,624,724,651
$\vdots$	$\vdots$	$\vdots$

Table 2 gives the minimum prime, and the "starting point" for various Γ_k. The "starting point" is loosely defined as the smallest prime r in the partition for which G'_r "appears" to be infinite. The reason for using G'_r instead of G_r is to exclude starting points such as 11: G_{11} appears to be infinite, but only contains two elements from the partition containing 11. The starting points were identified as the smallest element p of each Γ_k for which $|G'_p| \geq 10000$. By way of comparison, the largest G_p proven finite during this search had less than 100 elements.

4. Generalizations. The digit sum and the alternating digit sum can be generalized as follows.

Let ω be the root $\cos(2\pi/n) + i\sin(2\pi/n)$ of the nth cyclotomic polynomial $\Phi_n(x)$, and let $\mathbb{Z}[\omega]$ be the ring of algebraic integers of the extension field $\mathbb{Q}(\omega)$ of $\mathbb{Q}$. We shall concentrate here primarily on the case where $\mathbb{Z}[\omega]$ is a unique factorization domain. Define the *ω-digit sum $p\delta = \delta^b_\omega(p)$* to be

$$\sum_{k=0}^{m} e_k\omega^k,$$

where $p = e_0b^0 + e_1b^1 + \ldots + e_mb^m$ is the base b representation of p (p need not be a prime number here).

It is desirable to find a map $\psi : \mathbb{Z}[\omega] \to \mathbb{Z}_r = \mathbb{Z}/r\mathbb{Z}$ for some r, such that $p\delta\psi = 0 + r\mathbb{Z}$ if and only if $r \mid p$. Then a walk through the prime maze becomes a walk through $\mathbb{Z}[\omega]$, with each step of length 1, and $\ker\psi \subseteq \mathbb{Z}[\omega]$ becomes a set of forbidden points in the latter walk, just as the multiples of primes dividing of $b-1$ or $b+1$ were forbidden points when ω was 1 or -1.

To achieve this goal, let $k = \phi(n)$ be the degree of $\Phi_n(x)$, and let r be a divisor of $\Phi_n(b)$. Any element of $\mathbb{Z}[\omega]$ may be uniquely written as $\chi = e_0 + e_1\omega + \ldots + e_{k-1}\omega^{k-1}$. Let ψ map χ to $e_0 + e_1b + \ldots + e_{k-1}b^{k-1} + r\mathbb{Z}$.

4.1. Theorem. *The map ψ defined above is a well defined ring homomorphism. Furthermore, for $p \in \mathbb{Z}$, $r \mid p$ if and only if $p\delta \in \ker\psi$.*

Proof. Certainly it is well defined. It is easy to show that it preserves addition. Now, if $\chi_1 = e_0 + e_1\omega + \ldots + e_{k-1}\omega^{k-1} = e(\omega)$ and $\chi_2 = f_0 + f_1\omega + \ldots + f_{k-1}\omega^{k-1} = f(\omega)$ are such that $\chi_1\chi_2 = g_0 + g_1\omega + \ldots + g_{k-1}\omega^{k-1} = g(\omega)$ where $e(x), f(x), g(x) \in \mathbb{Z}[x]$, it can only be because the cyclotomic polynomial $\Phi_n(x)$ divides $g(x) - (ef)(x)$ in the polynomial ring $\mathbb{Z}[x]$. It follows then that $\Phi_n(b)$ divides $g(b) - (ef)(b)$, whence $(\chi_1\psi)(\chi_2\psi) = (\chi_1\chi_2)\psi$ as required.

Now, if $p = e_0 + e_1b + \ldots + e_mb^m$, then $p\delta\psi = e_0 + e_1b + \ldots + e_mb^m + r\mathbb{Z} = p + r\mathbb{Z}$, so $p\delta\psi = 0 + \mathbb{Z}$ if and only if r divides p, as required. ∎

As an example, let $n = 4$, so that $\omega = i = \sqrt{-1}$, and $\mathbb{Z}[\omega]$ becomes the Gaussian integers $\mathbb{Z}[i]$. The cyclotomic polynomial $\Phi_n(x)$ in this case is x^2+1, so if $b = 2$, we must use $r = 5$. Let $c+id \in \mathbb{Z}[i]$. Then $(c+id)\psi = c+2d$, which is a multiple of 5 if and only if $c + 2d$ is a multiple of the Gaussian prime $1 + 2i$. A walk through G_1 must avoid numbers $p > 5$ such that $1 + 2i$ divides $\delta^2_i(p)$.

At first glimpse, this is not a very useful fact. Consideration of δ^b_1 and δ^b_{-1} yielded powerful results because the corresponding cyclotomic polynomials $\Phi_1(x)$ and $\Phi_2(x)$ each have degree 1, so that the walk through $\mathbb{Z}[\omega]$ is through $\mathbb{Z}$ itself. Such a walk is already sufficiently constrained that the extra constraint(s) (that the walk must not touch $\ker\psi$) splits the maze into infinitely many partitions. Unfortunately, a walk in $\mathbb{Z}[i]$ has so much freedom that the restriction on $\delta^2_i(p)$ (that it should not be a multiple of $1+2i$) is not enough to help very much.

On the other hand, for any prime r not dividing b, r divides $b^{r-1}-1$, so that there exists some n dividing $r-1$ for which $r \mid \Phi_n(b)$. It follows that any condition of the form "r must not divide p" can be expressed in the form "$\delta^b_\omega(p)$ must not be in $\ker\psi$", for some ω, no matter what the base b under consideration. Therefore, the above analysis (almost) completely captures the structure of the prime number maze (except that $\delta^b_\omega(p)$ is permitted to touch $\ker\psi$ for the one exception $p = r$).

Furthermore, for at least some bases b, these results do produce some "useful" partitioning theorems. A method for finding them is illustrated in Section 5, after the following lemmas and theorem.

4.2. Lemma. *Let n be such that $\mathbb{Z}[\omega]$ is a unique factorization domain, let r be a prime integer dividing $\Phi_n(b)$, and define the maps $\delta = \delta^b_\omega$ and ψ as before. Then r factorizes over $\mathbb{Z}[\omega]$, and $\chi\psi = 0 + r\mathbb{Z}$ for precisely one of its irreducible factors* (*up to associates*).

Proof. Now, if $\chi_1\psi = \chi_2\psi = 0 + r\mathbb{Z}$, then $\mathrm{GCD}(\chi_1,\chi_2)\psi = 0 + r\mathbb{Z}$ also, which leads to a contradiction if $\mathrm{GCD}(\chi_1,\chi_2)$ is a unit of $\mathbb{Z}[\omega]$. Since $r\psi = (b-\omega)\psi = 0 + r\mathbb{Z}$, and $b-\omega$ is not a multiple of r, it follows that r is not irreducible in $\mathbb{Z}[\omega]$. Let $r = \chi_1\chi_2\dots\chi_l$ be a factorization of r in $\mathbb{Z}[\omega]$ into irreducibles. It follows that $\chi_i\psi = 0 + r\mathbb{Z}$ for exactly one of the χ_i. It must be the case for at least one, since $(\chi_1\psi)(\chi_2\psi)\dots(\chi_l\psi) = 0 + r\mathbb{Z}$, and $\mathbb{Z}_r$ is a field (r being prime in $\mathbb{Z}$). If $\chi_i\psi = \chi_j\psi = 0 + r\mathbb{Z}$, where χ_i and χ_j are not associates, then the fact that $\mathrm{GCD}(\chi_i,\chi_j)$ is a unit leads to a contradiction. ∎

4.3. Lemma. *Let n be as before, let r be a prime integer dividing $\Phi_n(b)$, and let χ be an irreducible factor of r in $\mathbb{Z}[\omega]$. Let G be the Galois group of $\mathbb{Q}(\omega)$, and let $X = \chi^G$ be the orbit of χ under the action of the Galois group. Then $r = \prod_{\zeta\in X}\zeta$.*

Proof. First of all, let χ divide r. Then, for any element α of the Galois group, $\chi\alpha$ divides $r\alpha = r$. Hence every element of X divides r, so $\prod_{\zeta\in X}\zeta$ divides r. If r has some additional nontrivial factor υ, then letting $Y = \upsilon^G$, we find that $(\prod_{\zeta\in X}\zeta)(\prod_{\upsilon\in Y}\upsilon)$ divides r, contradicting the choice of r as a prime integer. ∎

4.4. Theorem. *Let n and r be as before, and let ψ_b be the map ψ defined earlier, with $\omega\psi_b = b+r\mathbb{Z}$. Then for each irreducible factor χ of r there exists b' such that $\chi\psi_{b'} = 0 + r\mathbb{Z}$.*

Proof. From Lemma 4.2, there exists χ_1 such that $\chi_1\psi_b = 0 + r\mathbb{Z}$, and from Lemma 4.3, there exists an element α of the Galois group of $\mathbb{Q}(\omega)$ such that $\chi\alpha = \chi_1$. Now α sends ω to a primitive nth root of unity, that is, $\omega\alpha = \omega^i$ for some i with $\mathrm{GCD}(i, n) = 1$ (see Chapter 48 of [3], in particular Theorem 48.1). It follows that $\alpha\psi_b = \psi_{b^i}$, and hence, letting $b' \equiv b^i \bmod r$, that $\chi\psi_{b'} = \chi\psi_{(b^i)} = \chi\alpha\psi_b = \chi_1\psi_b = 0 + r\mathbb{Z}$, as required. ■

5. Some final partition theorems. The main motivation for the results of the previous section is to prove that the technique illustrated here will always work (at least when $\mathbb{Z}[\omega]$ is a unique factorization domain).

Let $n = 4$, that is, let $\omega = \sqrt{-1}$, so $\mathbb{Z}[\omega]$ is the set $\mathbb{Z}[i]$ of Gaussian integers. Figure 1 shows in black those Gaussian integers which are divisible by either $2 - i$, $3 - 2i$, $4 - i$, $5 - 2i$ or $4 - 5i$.

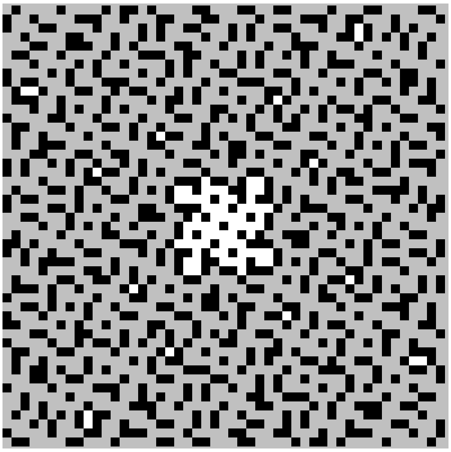

Fig. 1. The Gaussian integers

It will be noted that there is a pinwheel-shaped region centered at $0 + 0i$ which is separated from the rest of the plane by a "wall" of multiples of these primes. If we can find a base b for which $5 \mid (2 - b)$, $13 \mid (3 - 2b)$, $17 \mid (4 - b)$, $29 \mid (5 - 2b)$ and $41 \mid (4 - 5b)$, then we will have another proof of the following theorem.

5.1. Theorem. *For such a b, the base b maze has infinitely many disjoint partitions.*

Proof. Infinitely many, because even though the boundary of the pinwheel centered at $0+0i$ contains 5, the pinwheel pattern is repeated around every multiple in $\mathbb{Z}[i]$ of $(2-i)(3-2i)(4-i)(5-2i)(4-5i) = -966-617i$. ∎

The partitions derived from the pinwheel will be quite distinct from any partitions derived using Theorems 2.2 and 3.1 (digit sums or alternating digit sums).

Let us proceed to find such a base b. If b is as required, then b is a solution to the congruences

$$\begin{aligned} 2-b &\equiv 0 \bmod 5, &\quad \text{that is,} &\quad b \equiv 2 \bmod 5,\\ 3-2b &\equiv 0 \bmod 13, &\quad \text{that is,} &\quad b \equiv 8 \bmod 13,\\ 4-b &\equiv 0 \bmod 17, &\quad \text{that is,} &\quad b \equiv 4 \bmod 17,\\ 5-2b &\equiv 0 \bmod 29, &\quad \text{that is,} &\quad b \equiv 17 \bmod 29,\\ 4-5b &\equiv 0 \bmod 41, &\quad \text{that is,} &\quad b \equiv 9 \bmod 41. \end{aligned}$$

It follows that $b \equiv 1103032 \bmod 1313845$.

In fact, for some such bases b (in particular $b = 1103032 + 1313845k$, where $k = 26, 86, \ldots$), both $b+1$ and $b-1$ are prime, so that this analysis yields a partition theorem which is stronger (in some sense) than either of Theorems 2.2 or 3.1.

As a bonus, this figure also shows some points (namely $6+14i$, $10+7i$ and their associates) which are completely surrounded by black. These yield the equivalent of Brier numbers in these bases. Specifically, if $\delta_i^b(k) = 6+14i$ or $10+7i$, then $k \pm b^m$ is composite for any m, and from whence it may be shown that $k \cdot b^n \pm 1$ is also composite for any n. The smallest such example is $k = 7721234$ for $b = 1103032$, so that $7721234 \cdot 1103032^n \pm 1$ is always composite, being divisible by one of 5, 13, 17, 29 or 41. Note that one should not expect that all Brier numbers for all bases will be obtainable in this way.

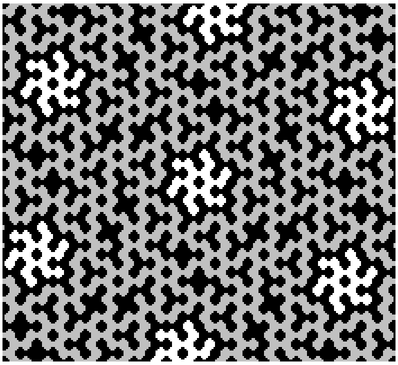

Fig. 2. The Eisenstein integers

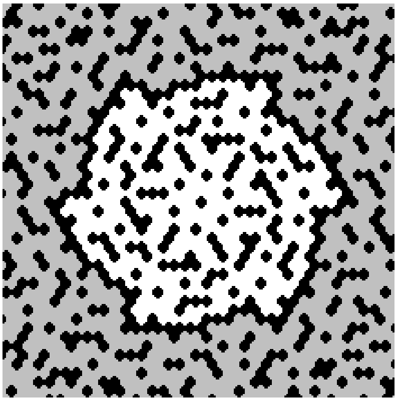

Fig. 3. The Eisenstein integers again

Alternatively, by considering the complex conjugate diagram to Figure 1, one can deduce partition theorems for bases of the form $b = 210813 + 1313845k$. There are twin primes $b \pm 1$ for b of this form when $k = 15, 39, 183, \dots$, and one may obtain the generalized Brier number 1264892 for $b = 210813$.

Figures 2 and 3 show elements of $\mathbb{Z}[\omega]$, where $\omega = \frac{1}{2}(1 + i\sqrt{3})$ is a primitive sixth root of 1 (the so-called Eisenstein integers). In Figure 2, the black dots are those elements which are multiples of either $1 + \omega$, $1 + 2\omega$ or $3 + \omega$. Again, there are repeated pinwheels isolated from the rest of $\mathbb{Z}[\omega]$ by walls of multiples. This provides a partition theorem for bases b satisfying $3 \mid (1 + b)$, $7 \mid (1 + 2b)$ and $13 \mid (3 + b)$, that is, b is of the form $b = 101 + 273k$. Alternatively, since $\mathbb{Z}[\omega] = \mathbb{Z}[\omega^2]$ and ω^2 is a primitive cube root of 1, we can write $1 + \omega = 2 + \omega^2$, $1 + 2\omega = 3 + 2\omega^2$ and $3 + \omega = 4 + \omega^2$, and then find a partition theorem for bases b satisfying $3 \mid (2 + b)$, $7 \mid (3 + 2b)$ and $13 \mid (4 + b)$, that is, $b = 100 + 273k$.

In fact, $\Phi_3(100) = 10101 = 3 \cdot 7 \cdot 13 \cdot 37$, so if we let $b = 100$ and $r = 37$ and define the map ψ as before, there exists also a factor α of 37 in $\mathbb{Z}[\omega^2]$ for which $\alpha\psi = 0 + 37\mathbb{Z}$. The factor in question may be taken to be $7 + 4\omega^2$. Adding all multiples of $7 + 4\omega^2$ to Figure 2 would reveal some isolated points in the prime number maze, leading also to generalized Brier numbers for base 100. The smallest generalized Brier number obtainable in this way is 926. It should be noted that this is by no means the smallest generalized Brier number for base 100, which is 10 (or 43, if one insists that $k \cdot b^n \pm 1$ be composite for $n = 0$ also).

Figure 3 shows a larger pinwheel bounded by multiples of $2 + \omega$, $1 + 3\omega$, $1 + 5\omega$, $4 + 3\omega$, $6 + \omega$, $4 + 5\omega$, $6 + 7\omega$, $9 + 5\omega$, $1 + 12\omega$ and $11 + 3\omega$. It is included to show that multiples of $1 + \omega$ are not strictly necessary. The solution of the resulting system(s) of congruences is left as an exercise.

The author readily admits that few human beings are likely to explore the base 1103032 or 210813 prime number maze as a form of recreation or for any pragmatic purpose (although the fortuitous base 100 theorem may be of some interest). The same methods could be applied to find partition theorems based on any cyclotomic extension $\mathbb{Z}[\omega]$. For higher-degree extensions, more irreducibles will be needed, in general making the obtained base even higher. It seems unlikely to this author that for the base 2 maze, any useful partition theorem beyond Theorem 3.1 can be obtained.

6. Concluding remarks. There are other questions that may be worth investigating. The base b maze was defined so that at every step, one digit was changed by ±1. One could also define the mazes by allowing larger changes. For example, at each step we could allow a digit to change by $\pm t$, for any $0 < t \leq k \leq b-1$ (k fixed). Or, we could define a maze on the Gaussian primes, allowing at each step a change in one of the digits of either the real or the imaginary part.

Some other somewhat similar explorations were suggested by the referee. For example, if we allow digits to be added and removed, but not changed, we obtain what are called "truncatable" primes. A prime is *left-truncatable* if one can delete any number of its lead digits, and still obtain a prime. Similarly defined are *right-truncatable* primes. A *deletable* prime is one where for any k less than the number of its digits, we can remove some set of k digits and still have a prime. There are only finitely many left- and right-truncatable primes, but it is conjectured that the number of deletable primes is infinite. See [1] or [2] for information about these (and other) numbers.

The referee also pointed out some references to the "Gaussian Moat Problem". If one defines a walk on the primes such that at each step from p_1 to p_2 has $|p_1 - p_2|$ less than some fixed length, the walk is bounded, since arbitrarily large gaps exist in the primes. The equivalent problem is unsolved on the Gaussian primes, although some work has been done on it (see [4], [5] and [7]). However, there is apparently no work published on the "Eisenstein Moat Problem". It seems that whatever techniques eventually solve the former, they will likely apply just as well to the latter.

References

[1] C. Caldwell, *Truncatable primes*, J. Recreational Math. 19 (1987), 30–33.

[2] L. E. Card, *Patterns in primes*, ibid. 1 (1968), 93–99.

[3] J. B. Fraleigh, *A First Course in Abstract Algebra*, Addison-Wesley, 1982.

[4] E. Gethner and H. M. Stark, *Periodic Gaussian moats*, Experiment. Math. 6 (1997), 289–292.

[5] E. Gethner, S. Wagon and B. Wick, *A stroll through the Gaussian primes*, Amer. Math. Monthly 105 (1998), 327–337.

[6] W. Paulsen, *The prime number maze*, Fibonacci Quart., to appear.
[7] I. Vardi, *Prime percolation*, Experiment. Math. 7 (1998), 275–289.

Sepang Institute of Technology
Level 5, Klang Parade
2112 Jalan Meru
Klang, 41050, Selangor, Malaysia
E-mail: Michael.Hartley@sit.edu.my

Received on 12.7.2001
and in revised form on 23.1.2002 (4066)