Some Notes on Pollard's Rho-Method

by

Kevin Ford
California State University, Chico

August 10, 1989

Overview of the Rho-Method

In 1975, J. M. Pollard introduced a Monte Carlo method for finding small factors of integers, commonly known as the rho-method. His idea was to iterate a function, creating a sequence of integers (S_k) which behave "randomly". A factor of N is found when $\gcd(S_j-S_i,N) \neq 1$. Since a prime factor P will be found when $S_j \equiv S_i \pmod{P}$, it is desirable to minimize the number of iterations necessary for this. If the sequence (S_k) behaves randomly modulo P, then a repetition should occur on average in $1.03\sqrt{P}$ iterations [1]. Empirical evidence suggests that the sequence

$$S_0=x, \quad S_{i+1}=S_i^2+y, \quad y\neq 0,-2 \tag{1}$$

satisfies the randomness condition, but until very recently little was known why.

My goal was to try to determine why this sequence behaves randomly, so I started by gathering data on when the sequence repeats modulo various primes. The following three graphs illustrate the behavior of this sequence. The first shows the average and maximum iterations needed before a repetition is encountered modulo P, using all possible values of x and y. The sharp peaks on the maximum curve are due to the y=0 and y=-2 cases. The second graph depicts the percentage of pairs (x,y) which yield a repetition modulo P in fewer than $\sqrt{P}$ iterations. The third graph shows, for x=5, the number of iterations necessary for a repetition as a function of y, averaged over all primes < 40,000. Here, Floyd's cycle finding algorithm was used, which only checks for $S_{2i} \equiv S_i \pmod{P}$. The undesirability of y=0 and y=-2 is clear.

Why y=0 and y=-2 Don't Work

When y=0 or -2, the terms in the sequence (S_i) can be written as the 2^i-th terms in a two term linear recurrence. Because of this, the sequence (S_i) repeats in approximatly $O(P)$ rather that $O(\sqrt{P})$ iterations.

With y=-2, $S_i = \alpha^{2^i} + \alpha^{-2^i} = w_{2^i}$, where $w_0=2$, $w_1=x = \alpha+\frac{1}{\alpha}$, $w_{i+2}=\left(\alpha+\frac{1}{\alpha}\right)w_{i+1} - w_i$. Let a and k be the smallest integers for which $w_{a+k}\equiv w_a \pmod P$. It is known that k is approximately $O(P)$. To obtain a repetition in (1), $S_{c+h}\equiv S_c \pmod P$, we need $w_{2^{c+h}}\equiv w_{2^c} \pmod P$, or $2^c(2^h-1)\equiv 0 \pmod k$. If we choose c such that $2^c > k$, then the smallest h which satisfies this condition is $h=\mathrm{ord}_f 2$, where $k=2^m f$, f odd. Since $h \approx O(k) \approx O(P)$, the sequence (S_k) repeats in $O(P)$.

With y=0, we have $S_i = x^{2^i}$. A repetition in (S_k) will occur when $x^{2^j} \equiv x^{2^i} \pmod P$, or when $2^i(2^{j-i} -1)\equiv 0 \pmod k$, where $k=\mathrm{ord}_P x$. As in the y=-2 case, this leads to an $O(P)$ estimate for j-i.

It turns out that y=0 and y=-2 are the only y values which yield a nice linear recurrence relation which can be used to generate the sequence (S_k).

Recent Results

In a recent paper, Eric Bach [2] showed that for a fixed k, the probability of a repetition in (1) by the k^th iteration is at least $\binom{k}{2}/P + O(P^{-3/2})$ as $P\to\infty$, and that the probability of a repetition by $\lfloor\frac{1}{4}\log_2 P\rfloor$ iterations is $\Omega(\log^2 P)/P$. These are the best results known, but are still far from the desired results.

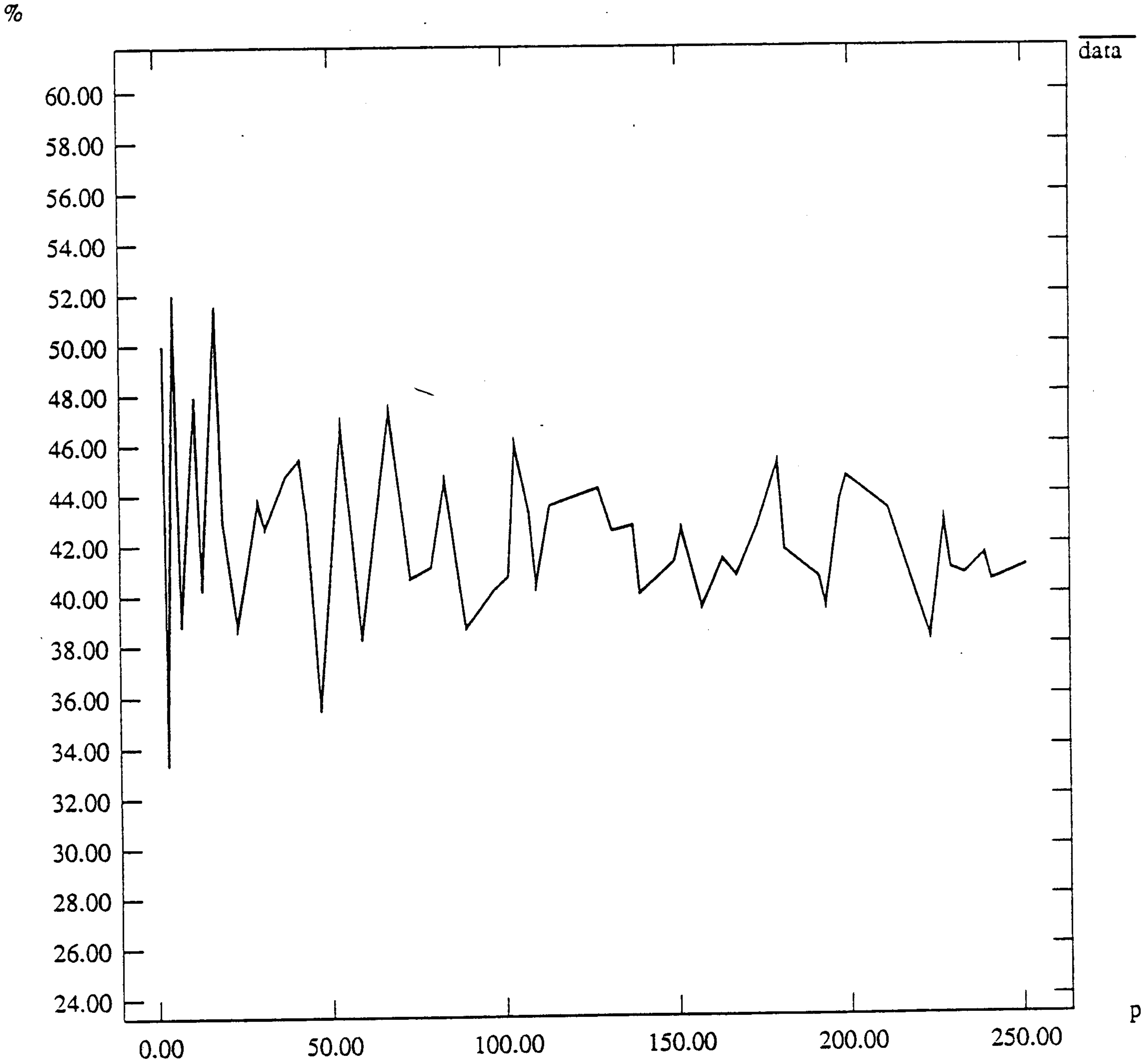
Bach formalizes the rho-method by defining **polynomials** $f_i \in Z[x,y]$ by

$$f_0=x, \quad f_{i+1}= f_i^2+y$$

He then defines a set of polynomials $\rho_{i,j}(x,y)$, each uniquely determined by the following:

1) $\rho_{i,j}$ is an irreducible divisor of $f_j - f_i$.
2) $\rho_{i,j}(\omega_{i,j},0) = 0$, where $\omega_{i,j}$ is a primitive 2^j-2^i-th root of unity.

Percent of Cycles Found Before Sqrt(p)



of f_i's in the same way the cyclotomic polynomials $\Phi_j(x)$ are constructed. From known relations

$$\prod_{d|j}\Phi_d(x) = x^j - x^0 \qquad \text{and} \qquad \Phi_j(x) = \prod_{d|j}(x^j - x^0)^{\mu(j/d)} ,$$

where $\mu(x)$ is the Möbius function, I derived

$$\rho_{0,j} = \prod_{d|j}(f_d - f_0)^{\mu(j/d)} \qquad \text{and} \qquad \rho_{i,j} = \prod_{d|j-i}(f_{i-1+d} + f_{i-1})^{\mu(\frac{j-i}{d})} \tag{5}$$

which can be seen by replacing x^j by f_j or f_{j+i-1}. Using (5), $f_i(x,y) = f_{i-1}(x^2+y,y)$ and $f_i(x,y) = f_i(-x,y)$ for $i \geq 1$, I discovered that

$$\rho_{1,j+1}(x,y) = \rho_{0,j}(-x,y) \tag{6}$$

and

$$\rho_{i+1,j+1}(x,y) = \rho_{i,j}(x^2+y,y) \ , \ i \geq 1 \tag{7}$$

Combining (6) and (7) yields

$$\rho_{i,i+j}(x,y) = \rho_{0,j}(-f_{i-1}(x,y),y) \ , \ i \geq 1$$

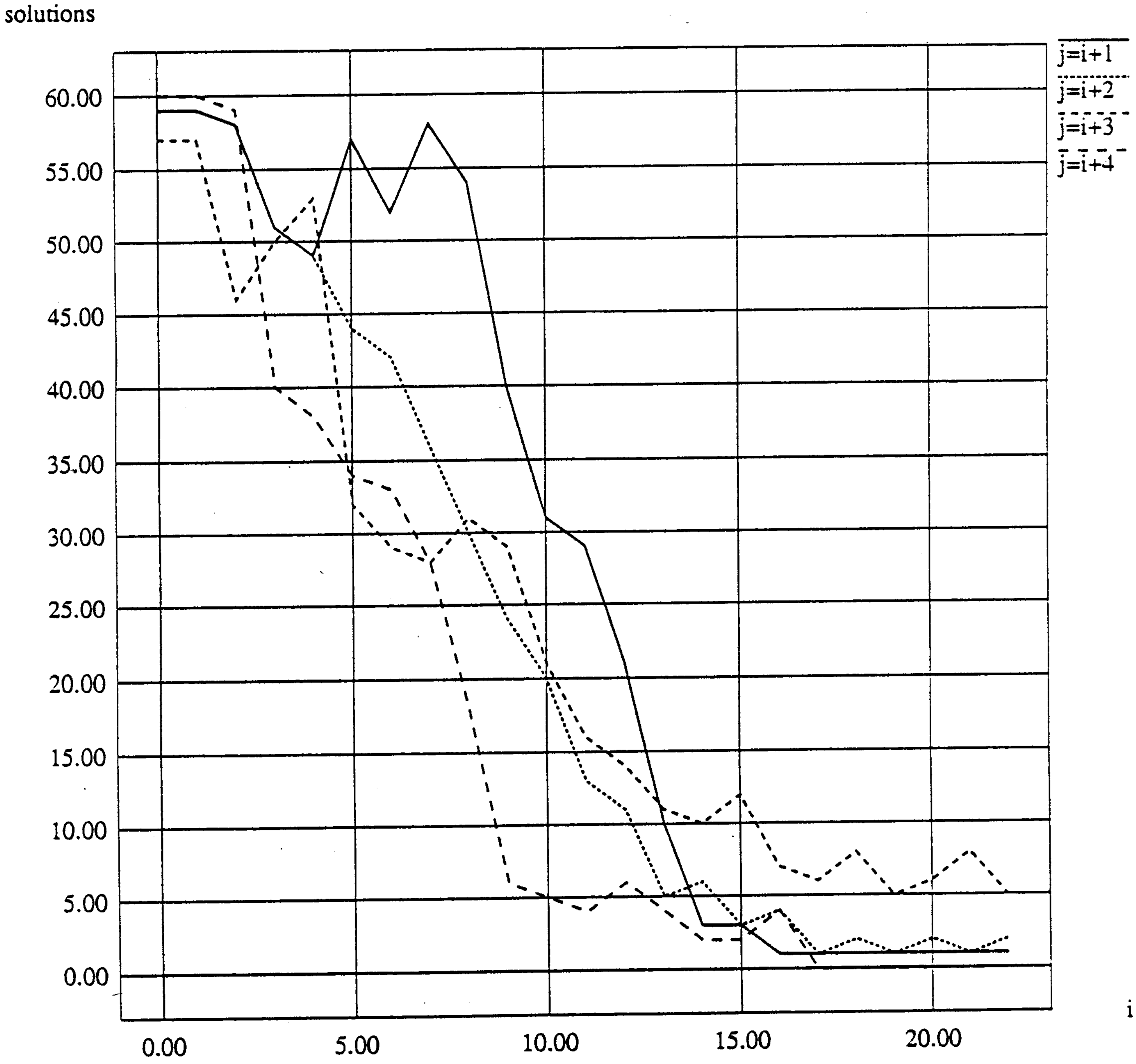
This makes computing values of ρ-polynomials with large indices and a small index difference very easy. More importantly, it provides an algorithm for constructing the solution set of $\rho_{i,i+j}(x,y) \equiv 0 \pmod{P}$ from the solution set of $\rho_{0,j}(x,y) \equiv 0 \pmod{P}$. Let $S_{i,j}$ represent the solution set of $\rho_{i,j}(x,y) = 0 \pmod{P}$. Then we have

$$S_{1,j+1} = \{ \ (x,y) \mid (-x,y) \in S_{0,j} \ \}$$

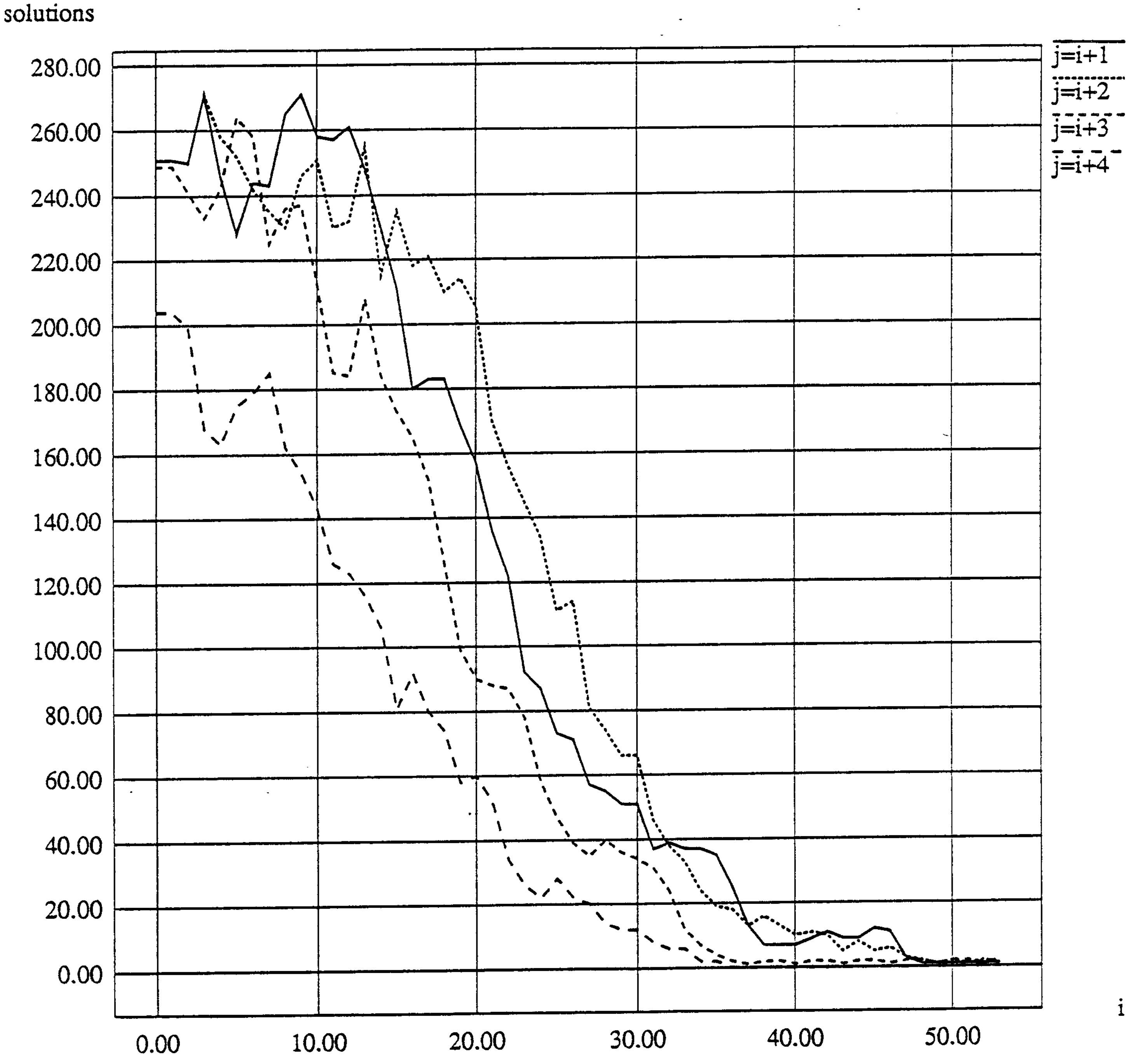
$$S_{i+1,j+1} = \{ \ (x,y) \mid (x^2+y,y) \in S_{i,j} \ \}$$

Looking at it another way, if $(x,y) \in S_{i,j}$, and x-y is a quadratic residue modulo P, then (x,y) "generates" the two solutions (s,y), $(-s,y) \in S_{i+1,j+1}$

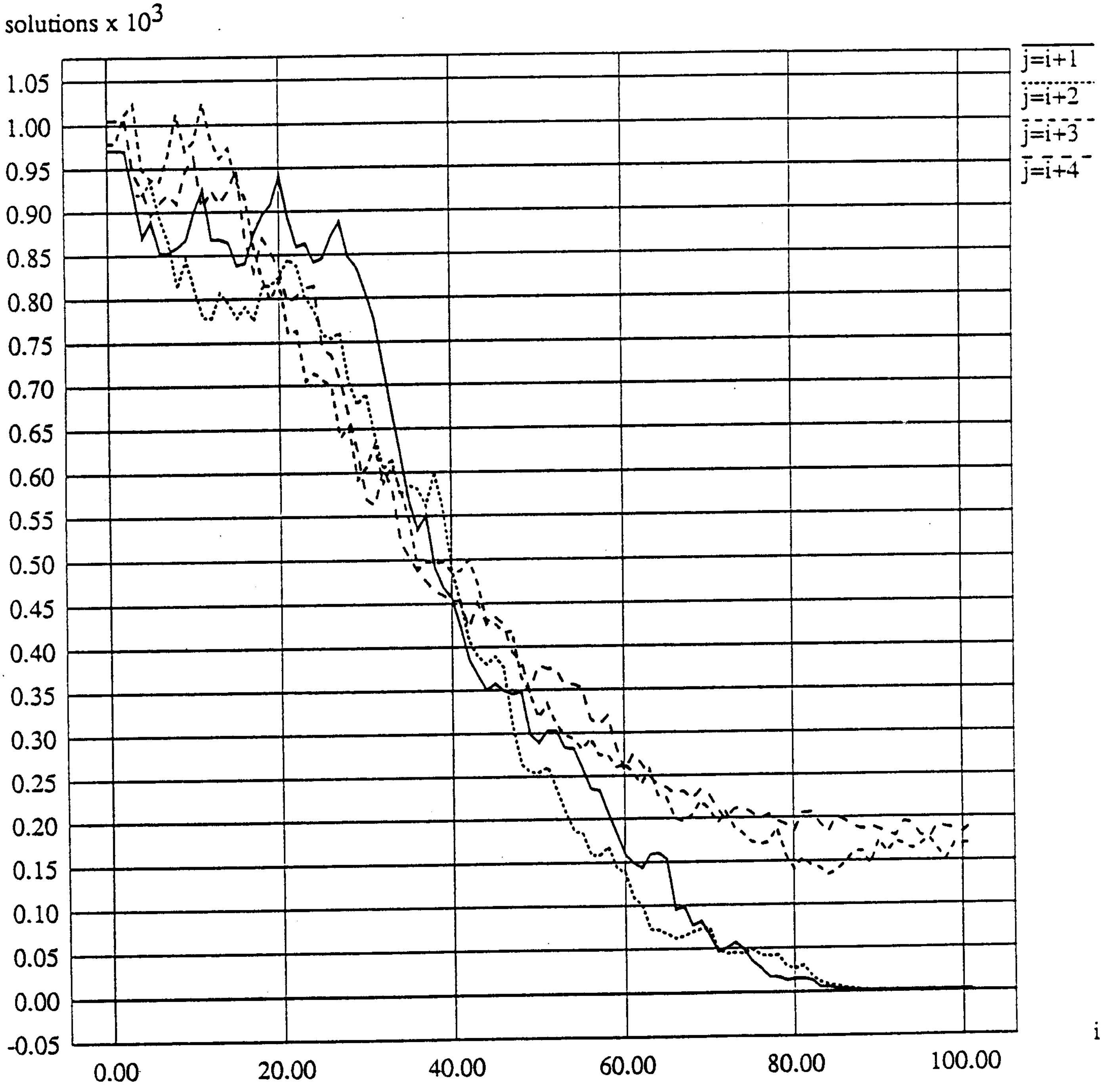
Solutions to rho_i,j(x,y)=0 (mod 59)



Solutions to rho_i,j(x,y)=0 (mod 251)



Solutions to rho_i,j(x,y)=0 (mod 971)


solutions x 10^3
i
j=i+1
j=i+2
j=i+3
j=i+4