SQUAREFREE VALUES OF POLYNOMIALS ALL OF WHOSE COEFFICIENTS ARE 0 AND 1

Michael Filaseta and Sergey Konyagin

Abstract: A squarefree number is a positive integer not divisible by the square of a prime. Are there infinitely many squarefree numbers all of whose binary digits are 0 and 1? If you don't know the answer to this question, this isn't the paper for you.

The title of this paper is deliberately ambiguous. Does it refer to squarefree polynomials $f(x)$ or to squarefree numbers $f(m)$? The paper deals with both of these issues. For n a non-negative integer, let

$$S_n = \{f(x) = \sum_{j=0}^{n} \epsilon_j x^j : \epsilon_j \in \{0,1\} \text{ for each } j \text{ and } \epsilon_0 = 1\}.$$

The condition $\epsilon_0 = 1$ insures that the elements of S_n are not divisible by x in $\mathbb{Q}[x]$. Let

$$S = \bigcup_{n=0}^{\infty} S_n.$$

One result we establish is:

Theorem 1. *Let $b = 3$, 4, or 5. Then there are infinitely many polynomials $f(x) \in S$ for which $f(b)$ is squarefree. Moreover, for such b, the density of polynomials $f(x) \in S$ for which $f(b)$ is squarefree is*

$$\lim_{n\to\infty} \frac{|\{f(x) \in S_n : f(b) \text{ is squarefree}\}|}{2^n} = \frac{6}{\pi^2} \prod_{p|b} \left(1 - \frac{1}{p^2}\right)^{-1}.$$

In particular, it follows that in each of the bases 3, 4, and 5, there are infinitely squarefree numbers all of whose digits are 0 and 1. A second result we obtain is:

Theorem 2. *Almost all polynomials in S are squarefree. In other words,*

$$\lim_{n\to\infty} \frac{|\{f(x) \in S_n : f(x) \text{ is squarefree}\}|}{2^n} = 1.$$

A much stronger result than Theorem 2 is believed to be true. Odlyzko has conjectured that almost all polynomials in S are irreducible, but this seems rather difficult to establish.