6-1-2007

The Probability of Relatively Prime Polynomials

Arthur T. Benjamin
Harvey Mudd College

Curtis D. Bennett
Loyola Marymount University

The Probability of Relatively Prime Polynomials

ARTHUR T. BENJAMIN
Harvey Mudd College
Claremont, CA 91711
benjamin@hmc.edu

CURTIS D. BENNETT
Loyola Marymount University
Los Angeles, CA 90045
cbennett@lmu.edu

Euclid does integers

The Euclidean algorithm for finding greatest common divisors, one of the oldest algorithms in the world, is also one of the most versatile. When applied to integers, Euclid's theorem can be stated as:

$$\text{If } a = qb + r \text{ then } \gcd(a, b) = \gcd(b, r).$$

The one sentence proof is that any number that divides a and b must also divide b and r (since $r = a - qb$) and vice versa; hence, the pairs (a, b) and (b, r) have the exact same set of common divisors. What turns this theorem into an algorithm is that if $b > 0$, then we can find a unique quotient q so that $0 \leq r < b$, allowing us to repeat the process with the second coordinate decreasing to zero. That is, if $\gcd(a, b) = c$, then Euclid's algorithm will look like

$$\gcd(a, b) = \gcd(b, r) = \cdots = \gcd(c, 0) = c.$$

For example,

$$\gcd(422, 138) = \gcd(138, 8) = \gcd(8, 2) = \gcd(2, 0) = 2.$$

Better yet, we can keep track of the integer quotients at each step (for example, $q_1 = \lfloor \frac{422}{138} \rfloor = 3$) and remove the gcd label so the above calculation looks like

$$(422, 138) \xrightarrow{q_1=3} (138, 8) \xrightarrow{q_2=17} (8, 2) \xrightarrow{q_3=4} (2, 0) = 2.$$

Now in addition to working from left to right, we can run the algorithm from right to left by holding on to the quotients. That is, given the quotients $q_1 = 3, q_2 = 17, q_3 = 4$, we can start with $(2, 0)$ and (from $q_3 = 4$) derive that it came from $(8, 2)$, which (from $q_2 = 17$) came from $(138, 8)$ which (from $q_1 = 3$) came from $(422, 138)$. In other words, we can run Euclid's algorithm backwards to obtain "dilcuE's algorithm:" $(b, r) \xrightarrow{q} (qb + r, b)$. For example,

$$2 = (2, 0) \xrightarrow{q_3=4} (8, 2) \xrightarrow{q_2=17} (138, 8) \xrightarrow{q_1=3} (422, 138).$$

As a practice problem, let's find the unique pair of relatively prime integers (i.e., whose greatest common divisor is one) for which Euclid's algorithm produces quotients $q_1 = 2, q_2 = 3, q_3 = 5, q_4 = 8$. By dilcuE's algorithm, we have

$$1 = (1, 0) \xrightarrow{q_4=8} (8, 1) \xrightarrow{q_3=5} (41, 8) \xrightarrow{q_2=3} (131, 41) \xrightarrow{q_1=2} (303, 131).$$

Euclid does polynomials

What makes Euclid's algorithm so versatile is that it can also be applied to objects other than integers. For example, given two polynomials $a(x)$ and $b(x)$ with rational coefficients, we define their greatest common divisor $c(x)$ to be the monic polynomial of greatest degree for which $c(x)$ divides $a(x)$ and $b(x)$. Here, Euclid's theorem says

$$\text{If } a(x) = q(x)b(x) + r(x), \text{ then } \gcd(a(x), b(x)) = \gcd(b(x), r(x)).$$

(The proof is exactly as before, except we insert (x) after every term.) To turn this theorem into an algorithm, we note that if the degree of $b(x)$ is at least one, then by the division algorithm for polynomials, we can always find unique quotient polynomial $q(x)$ so that the degree of $r(x)$ is strictly less than the degree of $b(x)$; hence Euclid's algorithm is guaranteed to terminate with an ordered pair $(kc(x), z)$ for some rational numbers $k \neq 0$ and z, and some monic polynomial $c(x)$ of degree at least one. If $z = 0$, then $\gcd(a(x), b(x)) = \gcd(kc(x), 0) = c(x)$; If $z \neq 0$, then $a(x)$ and $b(x)$ are relatively prime. For example,

$$\begin{aligned}(x^3 + 4x^2 + 5x + 2, 2x^2 - 6x - 8) &\xrightarrow{\frac{1}{2}x+\frac{7}{2}} (2x^2 - 6x - 8, 30x + 30)\\ &\xrightarrow{\frac{1}{15}x-\frac{4}{15}} (30x + 30, 0)\end{aligned}$$

where, for example, the first step indicates that

$$x^3 + 4x^2 + 5x + 2 = \left(\frac{1}{2}x + \frac{7}{2}\right)(2x^2 - 6x - 8) + (30x + 30).$$

Since $\gcd(30x + 30, 0) = 30(x + 1)$, it follows that $\gcd(x^3 + 4x^2 + 5x + 2, 2x^2 - 6x - 8) = x + 1$. On the other hand, adding 15 to the constant term of $a(x)$ results in

$$\begin{aligned}(x^3 + 4x^2 + 5x + 17, 2x^2 - 6x - 8) &\xrightarrow{\frac{1}{2}x+\frac{7}{2}} (2x^2 - 6x - 8, 30x + 45)\\ &\xrightarrow{\frac{1}{15}x-\frac{3}{10}} \left(30x + 45, \frac{11}{2}\right),\end{aligned}$$

so the original polynomials are relatively prime, since the constant term, $11/2$, is not zero. As with the integers, we can reverse this procedure starting with the final pair of polynomials, and backtracking through the quotients to obtain the original pair. Notice that the Euclidean Algorithm works here, because the coefficients of all of the polynomials, including the quotient polynomials, are allowed to be rational. If all coefficients were restricted to be integers, we could not apply the Euclidean algorithm.

Things become more interesting when we look at the set $\mathbb{Z}_2[x]$ where all of the coefficients come from the set $\{0, 1\}$, and all of the coefficient arithmetic is performed modulo 2. For example, in $\mathbb{Z}_2[x]$, $(x + 1)^3 = x^3 + 3x^2 + 3x + 1 = x^3 + x^2 + x + 1$, and $(x + 1)(x^2 + x + 1) = x^3 + 2x^2 + 2x + 1 = x^3 + 1$. For the exact same reason as in the polynomial case, we can perform the Euclidean algorithm on polynomials from $\mathbb{Z}_2[x]$ too. (In fact, it's easier in $\mathbb{Z}_2[x]$ because all nonzero polynomials are monic, and subtraction is the same as addition.) For instance,

$$\begin{aligned}(x^3 + x^2 + x + 1, x^3 + 1) &\xrightarrow{q_1=1} (x^3 + 1, x^2 + x) \xrightarrow{q_2=x+1} (x^2 + x, x + 1)\\ &\xrightarrow{q_3=x} (x + 1, 0).\end{aligned}$$

Thus $\gcd(x^3 + x^2 + x + 1, x^3 + 1) = x + 1$, which agrees with our earlier calculations. Again, if we hold on to the quotients, we can reverse the process through dilcuE's algorithm.

Euclid does 1-to-1 correspondences

We now are ready ask the main question of this paper. *If we choose two polynomials at random from* $\mathbb{Z}_2[x]$*, then what is the chance that they are relatively prime?* In FIGURE 1, we have a 16 by 16 matrix representing every pair of polynomials of degree 3 or lower. (Notice that the number of polynomials of degree n is 2^n since the coefficient of n must be one, but every subsequent coefficient can be one or zero. Likewise the number of polynomials of degree less than n is also 2^n.) Every dark square represents an ordered pair of polynomials that are relatively prime. Every light square represents an ordered pair of polynomials that are not relatively prime. We have drawn thick lines separating polynomials of different degrees. Notice that except for the four squares in the lower-left corner representing the ordered pairs of constant polynomials, all other thick rectangles have an equal number of dark and light squares. As the next theorem shows, this is not a coincidence.

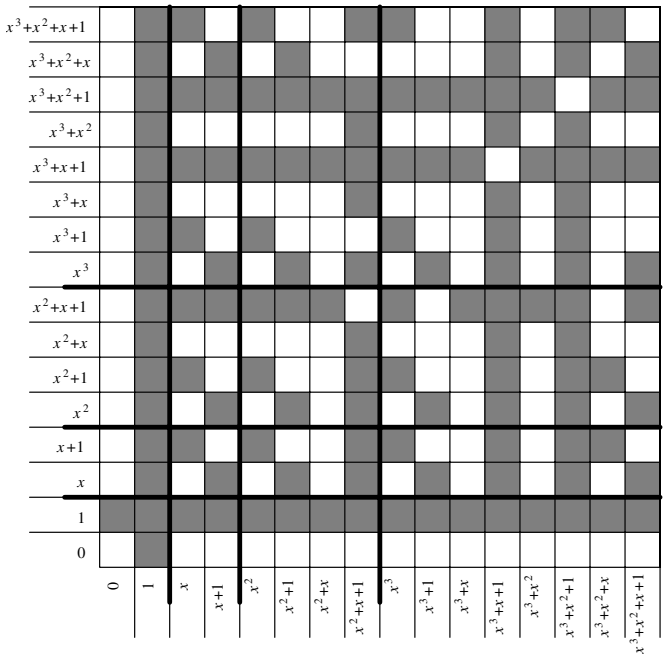

Figure 1 In every solid rectangle, except for the one in the lower left corner, half of the polynomials in $Z_2[x]$ are relatively prime (as represented by the dark squares). But how do you pair up the dark squares with the light squares?

THEOREM 1. *Let* $a(x)$ *and* $b(x)$ *be randomly chosen (i.e., uniformly and independently) from the set of polynomials in* $\mathbb{Z}_2[x]$ *of degree m and n, respectively, where m and n are not both zero. Then the probability that* $a(x)$ *and* $b(x)$ *are relatively prime is* $1/2$.

Proof. Without loss of generality, we assume that $m \geq n$. Our goal is to show that every relatively prime pair $(a(x), b(x))$ can be matched up with a non-relatively prime pair $(a_1(x), b_1(x))$, where a_1 and b_1 have the same degree as a and b, respectively.

If $n = 0$, then we match the relatively prime pair $(a(x), 1)$ with the non-relatively prime pair $(a(x), 0)$. Now suppose that $n \geq 1$ and let $(a(x), b(x))$ be a non-relatively prime pair. Then applying Euclid's algorithm gives us a unique sequence

$$(a(x), b(x)) \xrightarrow{q_1} (b(x), r_1(x)) \xrightarrow{q_2} (r_1(x), r_2(x)) \xrightarrow{q_3} \cdots \xrightarrow{q_t} (c(x), 0)$$

where $c(x)$, a polynomial of degree at least one, is the greatest common divisor. Starting with the relatively prime pair $(c(x), 1)$ and using the same quotient polynomials, $q_t, \ldots, q_1$, we can reverse Euclid's algorithm to produce a relatively prime pair $(a_1(x), b_1(x))$, which have the same degrees as $(a(x), b(x))$. ∎

For example, when $a(x) = x^3 + x^2 + x + 1$ and $b(x) = x^3 + 1$, the Euclidean algorithm produces the greatest common divisor $c(x) = x + 1$.

$$(x^3 + x^2 + x + 1, x^3 + 1) \xrightarrow{q_1=1} (x^3 + 1, x^2 + x) \xrightarrow{q_2=x+1} (x^2 + x, x + 1) \xrightarrow{q_3=x} (x + 1, 0).$$

Now running the Euclidean algorithm backwards from the relatively prime pair $(x + 1, 1)$, with the same quotients

$$(x + 1, 1) \xrightarrow{q_3=x} (x^2 + x + 1, x + 1) \xrightarrow{q_2=x+1} (x^3 + x, x^2 + x + 1) \xrightarrow{q_1=1} (x^3 + x^2 + 1, x^3 + x)$$

we obtain $(a_1(x), b_1(x)) = (x^3 + x^2 + 1, x^3 + x)$, which is a relatively prime pair since Euclid's algorithm reduces it to $(x + 1, 1)$.

COROLLARY 2. *If $a(x)$ and $b(x)$ are randomly chosen from the set of polynomials in $\mathbb{Z}_2[x]$ of degree less than n, then the probability that they are relatively prime is $\frac{1}{2} + \frac{1}{4^n}$.*

Proof. There are 2^n polynomials of degree less than n and therefore 4^n ordered pairs of polynomials $(a(x), b(x))$. Three of the four constant pairs $(0, 1)$, $(1, 0)$, $(1, 1)$ are relatively prime. From Theorem 1, among the remaining $4^n - 4$ pairs, exactly half of them are relatively prime. Thus the probability of a relatively prime pair is

$$\frac{3 + \frac{1}{2}(4^n - 4)}{4^n} = \frac{1}{2} + \frac{1}{4^n}.$$ ∎

In a recent paper [**1**], Corteel, Savage, Wilf, and Zeilberger prove a special case of Theorem 1 (under the assumption that $m = n$) by an elegant generating function argument, but ask for a "nice simple bijection that proves this result." We hope that our Euclidean bijection is nice and simple enough. We note that Reifegerste [**2**] also found a bijection using "resultant matrices" that was essentially the Euclidean algorithm in heavy disguise. As we'll see, the Euclidean bijection leads to interesting generalizations of Theorem 1 (some of which also appear in [**1**]).

Euclid does 1-to-many correspondences

What if the coefficients of our polynomial come from $\mathbb{Z}_3$ instead of $\mathbb{Z}_2$? A picture similar to FIGURE 1 would show that, except for the lower left corner of constant

polynomial pairs, in every thick rectangle, precisely two thirds of all polynomial pairs are relatively prime. (The polynomials are listed (from left to right and from bottom to top) in lexicographic order. For example, the first nine columns correspond to the polynomials: 0, 1, 2, x, $x+1$, $x+2$, $2x$, $2x+1$, and $2x+2$.)

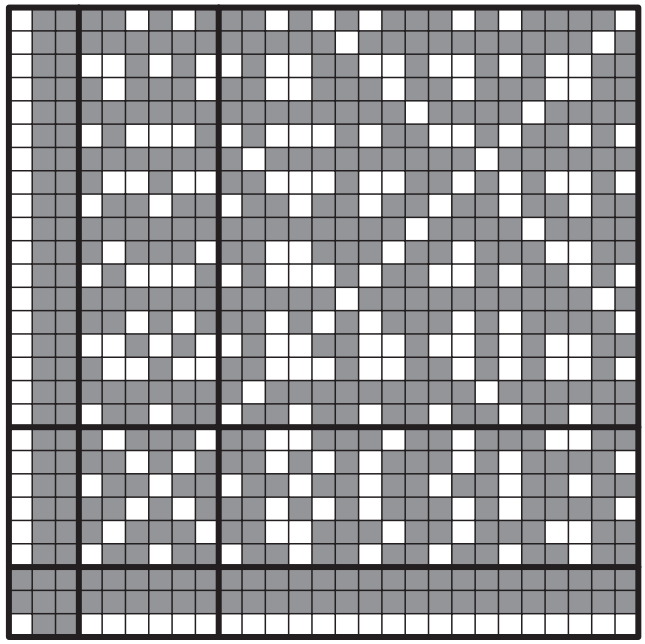

Figure 2 Every solid rectangle, except for the one in the lower left corner, has twice as many dark squares (representing relatively prime polynomials in $Z_3[x]$) as light squares. But how do you assign two dark squares to each light square?

In general, if our coefficients come from a finite field F of q elements (for instance, the set $F = \mathbb{Z}_q$, when q is prime) then we have the following generalization.

THEOREM 3. *Let F be a finite field of q elements, and let $a(x)$ and $b(x)$ be randomly chosen from the set of polynomials in $F[x]$ of degree m and n, respectively, where m and n are not both zero. Then the probability that $a(x)$ and $b(x)$ are relatively prime is $1 - 1/q$.*

Proof. To prove this, we show that for every non-relatively prime pair $(a(x), b(x))$, there are $q-1$ relatively prime pairs; hence the proportion of non-relatively prime pairs is $1/q$. If $n = 0$, then the non-relatively prime pair $(a(x), 0)$ is matched up with the $q-1$ relatively prime pairs $(a(x), z)$ where z is a nonzero element of F. (Note that $\gcd(2x, 2) = 1$, not 2, since 2 divides 1, and we insist that the greatest common divisor be monic.)

When $n \geq 1$, then we can apply Euclid's algorithm to $(a(x), b(x))$, producing a unique set of quotient and remainder polynomials,

$$(a(x), b(x)) \xrightarrow{q_1} (b(x), r_1(x)) \xrightarrow{q_2} (r_1(x), r_2(x)) \xrightarrow{q_3} \cdots \xrightarrow{q_s} (kc(x), z)$$

where $c(x)$ is a monic polynomial, and $k \neq 0$ and z are constants in F. If $z = 0$, then $a(x)$ and $b(x)$ have greatest common divisor $c(x)$; otherwise they are relatively prime.

Now suppose $n \geq 1$, and let $(a(x), b(x))$ be a non-relatively prime pair. Then Euclid's algorithm produces a unique set of quotient and remainder polynomials

$$(a(x), b(x)) \xrightarrow{q_1} (b(x), r_1(x)) \xrightarrow{q_2} (r_1(x), r_2(x)) \xrightarrow{q_3} \cdots \xrightarrow{q_s} (kc(x), 0)$$

where $c(x)$ is a monic polynomial of degree at least one, and k is a nonzero constant in F. Starting with $(kc(x), 0)$ and the quotients $q_s, \ldots, q_1$, we can reverse Euclid's algorithm to reconstruct $(a(x), b(x))$. Likewise, for each nonzero constant z in F, we can start with the relatively prime pair $(kc(x), z)$ and the same quotient polynomials $q_s, \ldots, q_1$ to produce a relatively prime pair $(a_z(x), b_z(x))$, which have the same degree as $a(x)$ and $b(x)$ respectively. Since there are $q - 1$ choices for z we have established the desired 1-to-$(q - 1)$ correspondence. ∎

For example, suppose that $q = 3$, $F = \mathbb{Z}_3$, $m = 5$, $n = 3$, and consider the pair $(x^5 + x, x^3 + x + 1)$. By Euclid's algorithm,

$$\begin{aligned}(x^5 + x, x^3 + x + 1) &\xrightarrow{q_1 = x^2 + 2} (x^3 + x + 1, 2x^2 + 2x + 1)\\ &\xrightarrow{q_2 = 2x + 1} (2x^2 + 2x + 1, 0)\end{aligned}$$

and so the pair is not relatively prime. Then starting with the relatively prime pairs $(2x^2 + 2x + 1, 1)$ and $(2x^2 + 2x + 1, 2)$, dilcuE's algorithm gives us two more relatively prime polynomials of degree 5 and 3, namely

$$\begin{aligned}(2x^2 + 2x + 1, 1) &\xrightarrow{q_2 = 2x + 1} (x^3 + x + 2, 2x^2 + 2x + 1)\\ &\xrightarrow{q_1 = x^2 + 2} (x^5 + x^2 + x + 2, x^3 + x + 2)\end{aligned}$$

and

$$\begin{aligned}(2x^2 + 2x + 1, 2) &\xrightarrow{q_2 = 2x + 1} (x^3 + x, 2x^2 + 2x + 1)\\ &\xrightarrow{q_1 = x^2 + 2} (x^5 + 2x^2 + x + 1, x^3 + x).\end{aligned}$$

The number of pairs of polynomials of degree less than n is q^{2n}. Among the q^2 constant pairs, all of them are relatively prime except for $(0, 0)$. (Yes, in $F[x]$, $\gcd(2, 2) = 1$.) Among the others, exactly $1/q$th of them are not relatively prime. Thus the number of nonrelatively prime pairs is $1 + \frac{1}{q}(q^{2n} - q^2)$. Dividing by q^{2n}, the probability of not being relatively prime is $\frac{1}{q} - \frac{q-1}{q^{2n}}$. Consequently, we have

COROLLARY 4. *Let F be a finite field with q elements. If $a(x)$ and $b(x)$ are randomly chosen from the set of polynomials in $F[x]$ of degree less than n, then the probability that they are relatively prime is $1 - \frac{1}{q} + \frac{q-1}{q^{2n}}$.*

Euclid does *m*-tuples

How about the probability that a random *triple* of polynomials in $F[x]$ is relatively prime? We claim that the probability that three polynomials $a_1(x), a_2(x), a_3(x)$ (not all constant) in $F[x]$ are not relatively prime is $1/q^2$. Without loss of generality, we'll assume that $a_1(x)$, $a_2(x)$, and $a_3(x)$ are chosen randomly from among polynomials of degree $d_1 \geq d_2 \geq d_3 \geq 0$, respectively, where $d_1 \geq 1$. The polynomials will not be relatively prime if and only if $a_1(x)$ and $a_2(x)$ are not relatively prime and

$\gcd(a_1(x), a_2(x))$ and $a_3(x)$ are not relatively prime. By Theorem 3, the probability that $a_1(x)$ and $a_2(x)$ are not relatively prime is $1/q$, and their gcd is a polynomial $c(x)$ with some degree $d \geq 1$. Given that $c(x)$ has degree d, Euclid's algorithm can be used (although we shall skip this detail) to show that it is equally likely to be any of the q^d monic polynomials of degree d. Applying Theorem 3 again, we have the probability that $c(x)$ and $a_3(x)$ are not relatively prime is also $1/q$. (Note that $a_3(x)$ is chosen independently of $c(x)$.) Multiplying the probabilities together, the probability that $a_1(x), a_2(x), a_3(x)$ are not relatively prime is $1/q^2$, and hence the probability that they are relatively prime is $1 - 1/q^2$.

Using induction, this argument can be extended to show

COROLLARY 5. *Let $(d_1, d_2, \ldots, d_m)$ be an ordered m-tuple of nonnegative integers (not all zero) and for $1 \leq i \leq m$, let $a_i(x)$ be a randomly chosen polynomial of degree d_i over $F[x]$, where F is a finite field with q elements. Then the probability that $a_1(x), a_2(x), \ldots, a_m(x)$ are relatively prime is $1 - \frac{1}{q^{m-1}}$.*

Finally, by a counting argument similar to the ones before, our final corollary is obtained.

COROLLARY 6. *If $a_1(x), \ldots, a_m(x)$ are randomly chosen polynomials of degree less than n in $F[x]$, where the field F has q elements, then the probability that they are relatively prime is $1 - 1/q^{m-1} + (q-1)/q^{mn}$.*

Using a similar argument, one can show that the set of pairs of *monic* polynomials of $\mathbb{Z}[x]$ can be partitioned into disjoint infinite sets, such that each set contains at most one pair that is not relatively prime. Thus, if a pair of monic polynomials is chosen at random (in an appropriate sense) from $\mathbb{Z}[x]$, then the probability that they are relatively prime is 1.

Acknowledgment. We thank Ed Scheinerman for bringing this problem to our attention and the referee for many valuable suggestions.

REFERENCES

1. S. Corteel, C. Savage, H. Wilf, D. Zeilberger, A Pentagonal Number Sieve, *Journal of Combinatorial Theory, Series A*, **82** (1998) No. 2, 186–192.
2. A. Reifegerste, On an Involution Concerning Pairs of Polynomials in $\mathbb{F}_2$, *Journal of Combinatorial Theory, Series A*, **90** (2000) 216–220.