THEOREM OF THE DAY

The Polynomial Coprimality Theorem *Among the m-tuples of monic polynomials of degree n over* GF(q), *the finite field with q elements, the proportion whose entries all share a non-trivial common factor is* $1/q^{m-1}$.

$$\mathrm{GCD}\left(x^8+x^7+x^2+1,\ x^8+1,\ (x+1)^8\right)$$
$$=\mathrm{GCD}\left((x^7+x+1)\times(x+1),\ (x+1)^8,\ (x+1)^8\right)$$
$$=(x+1)$$

$q = 2$
$m = 3$
$n = 8$

$n=2$	x^2	$x^2{+}1$	$x^2{+}x$	$x^2{+}x{+}1$
x^2				
$x^2{+}1$				
$x^2{+}x$				
$x^2{+}x{+}1$				

8 Coprime pairs 32

8 Non-coprime 32

$n=3$	•	•	•	•	•	•	•	•
•								
•								
•								
•								
•								
•								
•								
•								

$q=2,\ m=2,\ n=2,\ 3$

?

The triple $(x^8{+}x^7{+}x^2{+}1,\ x^8{+}1,\ (x{+}1)^8)$ consists of polynomials of degree 8. Their first coefficients are 1 (they are *monic*); if all their coefficients are interpreted as real numbers then, since the first two polynomials have no real roots, the entries of this triple can certainly share no common factor.

Easy red-yellow table facts ($q = m = 2$): (1) first row and column alternate: yellow/red; (2) main diagonal: all cells yellow; (3) table symmetrical about main diagonal; (4) irreducible polynomials: rows/columns all red except diagonal cells . . . none of which account for the circled red cell (which is $(x^3+x^2+x, x^3+x^2+x+1) = \left(x(x^2+x+1), (x+1)^3\right)$ — click the notes icon top right for more detail). . .

However, over the finite field GF(2), in which $1 + 1 = 0$, the polynomial $x + 1$ divides all three entries and is a non-trivial common factor. The theorem tells us that, for any fixed degree, precisely one quarter of such triples have non-trivial greatest common divisor (GCD). For $m = 2$, the proportion increases to 1/2, as illustrated in the two tables. For degree $n = 2$, the occurrences of coprime pairs are easily accounted for; degree three already presents one case which defies such simple analysis; for higher degrees, there is no obvious pattern.

This mysteriously simple result follows immediately from a miraculous ‘pentagonal number sieve’ devised by Sylvie Corteel, Carla D. Savage, Herbert S. Wilf and Doron Zeilberger, 1998. An elegant constructive proof was given by Arthur T. Benjamin and Curtis D. Bennett in 2007, neatly supplying, in the case $q = m = 2$, a bijection between coprime and non-coprime polynomial pairs.

Web link: blog.plover.com/math/prime-polynomials.html

Further reading: *Generatingfunctionology, 3rd revised ed.* by Herbert S. Wilf, A.K. Peters, 2006.