Mutual Primality and the Elementary Symmetric Functions

1 Introduction

Let's prove a simple theorem about mutual primality and the elementary symmetric functions. Let x_1 up to x_n be n variables, and let σ_1 up to σ_n be the n elementary symmetric functions on these variables, order irrelevant. We wish to show that whenever x_1 up to x_n are mutually prime (not necessarily pairwise), then so are σ_1 up to σ_n (the converse is trivial). To simplify notational matters, we will only consider the case $n = 3$, but the general case is virtually identical.

Suppose x, y and z are mutually prime. We will show that so are $x + y + z$, $xy + xz + yz$ and xyz. Suppose a prime p divides both xyz and $xy+xz+yz$. We will show it cannot divide $x+y+z$. Since $p \mid xyz$, p divides one of the factors, say $p \mid x$. Since $p \mid xy + xz + yz = x(y + z) + yz$, we see that $p \mid yz$. Again p must divide one of the factors, say $p \mid y$. However, from mutual primality, $p \nmid z$ and so $p \nmid x + y + z$.

Now let's see another proof for the case $n = 2$. Recall that $(x, y) = 1$ if and only if $ax + by = 1$ for some integers a and b. We start with a linear combination $ax + by = 1$ and produce a linear combination of $x + y$ and xy equaling unity:

$$\begin{aligned}1 &= (ax + by)^2 \\ &= a^2x^2 + b^2y^2 + 2abxy \\ &= a^2(x^2 + xy) + b^2(y^2 + xy) + (2ab - a^2 - b^2)xy \\ &= (a^2x + b^2y)(x + y) - (a - b)^2xy.\end{aligned}$$

Now we ask whether this can be done for more than two variables. That is, we ask whether there is in the ideal of $\mathbb{Z}[x_1, x_2, \ldots, x_n, a_1, a_2, \ldots, a_n]$ generated by the n symmetric functions on the first n variables a function of the form $P(\sum a_i x_i)$, where $P(\cdot)$ is a polynomial in one variable satisfying $P(1) = 1$[1]. In the next section we show that it is indeed the case.

2 Proof

First, we prove a Lemma: if the numbers x_1 up to x_n are relatively prime, then so are x_1^d up to x_n^d for any integer $d \geq 1$. We shall provide an explicit formula showing this. The proof is by induction. When $d = 1$ there is nothing to prove. Now suppose the claim is true for all $d-1$, and we'll prove it for d. We are given integers a_i such that $\sum a_i x_i = 1$, and other integers b_i such that $\sum b_i x_i^{d-1} = 1$. In order to find a linear combination in the x_i^ds totalling one, we shall look at powers of $\sum a_i x_i$. Each such power, when expanded, is a sum of monomials. We shall call a monomial *representable* if it is a linear combination in the x_i^ds. If all the monomials are representable, so is the power, and we are done.

When is a monomial representable? If it is divisible by x_i^d for some i then it is certainly representable. Next suppose the monomial is $\prod x_i^{d_i}$, where $d_i \geq 1$ for all i. When multiplied by any x_i^{d-1}, it becomes a multiple of x_i^d, hence representable. Thus $(\prod x_i^{d_i})(\sum b_i x_i^{d-1}) = \prod x_i^{d_i}$ is representable. Summarizing, a monomial is representable if either one of its powers is at least d, or none is zero. If we raise $\sum a_i x_i$ to a high enough power, we can guarantee that it happens: indeed, when raising to the $((d-1)(n-1)+1)$th power, each monomial has total degree $(d-1)(n-1)+1$. If the degrees are split among less than n variables, at least one will have degree at least d.

[1]In other words, we seek a formula of the form $\sum P_i \sigma_i$, where every P_i is a polynomial in the x_is and the a_is with integral coefficients, that equals one as long as $\sum a_i x_i = 1$.

Second, we use the Lemma to prove our Theorem. By the lemma, there are polynomial expressions a_1 up to a_n that satisfy $\sum a_i x_i^n = 1$. We will build an expression based on the elementary symmetric function equaling $\sum a_i x_i^n$. Our first summand is $\left(\sum a_i x_i^{n-1}\right)\left(\sum x_i\right)$. This gives us $\sum a_i x_i^n$ together with leftovers $a_i x_i^{n-1} x_j$. To get rid of these leftovers, we subtract $\left(\sum a_i x_i^{n-2}\right)\left(\sum x_i x_j\right)$. This gives us new leftovers of the form $a_i x_i^{n-2} x_j x_k$. Continuing this way, the penultimate step will create the leftovers $a_i \prod x_j$. These can be eliminated by adding or subtracting $\sum a_i \prod x_i$, completing the proof.

Let's see how all of this works in the first two cases. When $n = 2$, we need to show first that if x and y are mutually prime, then so are their squares. We are told to raise $ax + by = 1$ to the $(1 \cdot 1 + 1)$th power, giving $1 = (ax + by)^2 = a^2x^2 + b^2y^2 + 2abxy$. The first two terms are evidently representable. The third term is representable since $2abxy = 2abxy(ax+by) = 2a^2by \cdot x^2 + 2ab^2x \cdot y^2$. Putting it all together,

$$1 = (ax + by)^2 = a^2(1 + 2by)x^2 + b^2(1 + 2ax)y^2.$$

So we have c and d that satisfy $cx^2 + dy^2 = 1$. The final step is

$$1 = cx^2 + dy^2 = (cx + dy)(x + y) - (c + d)xy.$$

Next we move to $n = 3$. First we show that if x, y and z are mutually prime, then so are their squares. This time we are told to raise $ax + by + cz$ to the $(2 \cdot 1 + 1)$th power, giving us monomials of the forms x^3, x^2y and xyz. The first two are easy to represent, and the third can be represented as $xyz(ax + by + cz) = ayz \cdot x^2 + bxz \cdot y^2 + cxy \cdot z^2$.

The next step is to show that if x, y and z are mutually prime, then so are their cubes. Now we are obliged to raise $ax + by + cz$ to the fifth power. The resulting monomials are of the forms x^5, x^4y, x^3y^2, x^3yz and x^2yz. The first four are trivial to represent. To represent x^2yz, we use the fact that some A, B and C satisfy $Ax^2 + By^2 + Cz^2 = 1$. Then $x^2yz = x^2yz(Ax^2 + By^2 + Cz^2) = Axyz \cdot x^3 + Bx^2z \cdot y^3 + Cx^2y \cdot z^3$.

Now we are ready to the final step. Armed with α, β and γ that satisfy $\alpha x^3 + \beta y^3 + \gamma z^3$, we note that

$$1 = \alpha x^3 + \beta y^3 + \gamma z^3 = (\alpha x^2 + \beta y^2 + \gamma z^2)(x + y + z) - (\alpha x + \beta y + \gamma z)(xy + xz + yz) + (\alpha + \beta + \gamma)xyz.$$