35) Suppose we have two devices for producing random numbers from a chosen set. The first device produces the (nonnegative) integers \(a_1, \ldots, a_m\) (duplicates permitted) each with probability \(1/m\), the second device the numbers \(b_1, \ldots, b_n\) each with probability \(1/n\). (E.g. a standard die produces \(1, \ldots, 6\) each with probability \(1/6\).

a) We define two rational polynomials, \(f = \sum_{i=1}^{m} \frac{x}{m} a_i\) and \(g = \sum_{i=1}^{n} \frac{x}{n} b_i\). Assume that \(fg = \sum_{i} p_i x^i\). Show that \(p_i/(mn)\) is the probability that an independent run of both devices produces numbers that sum up to \(i\).

We now want to study how one could achieve certain probability distributions in different ways. For this we want to prescribe the product \(p = fg\) and determine whether this product can be obtained from polynomials \(f\) and \(g\), both of which can be written in the form \(\sum_{i=1}^{d} x^i\). We call such a polynomial \(d\)-termable. Because \(\mathbb{Z}[x]\) is a UFD, we can do this by looking at the factorization of \(p\) into irreducibles.

b) Suppose that \(p = (x^6 + x^5 + x^4 + x^3 + x^2 + x)^2\) (the sum probabilities when rolling two standard dice). We want to see whether the same sum probabilities can also be obtained by rolling two cubes which are differently labelled. Using the fact that

\[x^6 + x^5 + x^4 + x^3 + x^2 + x = x(x+1)(x^2+x+1)(x^2-x+1)\]

as a product of irreducibles. Determine all possibilities for factors \(f\) and \(g\), both with constant term \(0\) (i.e. no outcome would be \(0\)), that yield this particular \(p\) and can be written in the specified form. Show that there is one other pair of dice (called Sicherman dice), which will produce the same probabilities of sums.

Doing this by hand is getting tedious rather quickly and we want to use a computer. In GAP, the following function checks whether a polynomial \(f\) is \(d\)-termable:

```gap
dtermable:=function(f,d)
  f:=CoefficientsOfUnivariatePolynomial(f);
  return ForAll(f,i->i>=0) and Sum(f)=d;
end;
```

For a polynomial \(p\), the following function return all divisors of \(p\)

```gap
divisors:=p->List(Combinations(Factors(p)),x->Product(x,p^0));
```

With these commands, one could solve part b) for example in the following way:

```gap
gap> p:=(x+x^2+x^3+x^4+x^5+x^6)^2;;
gap> Filtered(divisors(p),i->dtermable(i,6) and Value(i,0)=0
and dtermable(p/i,6) and Value(p/i,0)=0);
```

c) Suppose we repeat b) but with standard labeled tetrahedra (faces 1-4), octahedra (faces 1-8) and dodecahedra (faces 1-20). Are there analogues of the Sicherman dice?

d') Now consider an equal distribution of the numbers 1 to 36. (I.e. \(p:=\text{Sum}([1..36],i->x^i)\)). Is it possible to produce this equal distribution with two cubes? If all faces are labelled positive? What about a dodecahedron and a tetrahedron?

e') Is there (apart from replacing one pair of dice with a pair of Sicherman dice) an analogue of Sicherman dice for rolling three dice?

36) Consider the following cube, whose corners we'll label with the numbers 1 to 8:
Write down permutations in cycle form that show how the corners change under the following operations.

a) Clockwise rotation by 90° around the axis (axis 1) that goes through the front and back side.

b) Rotation (by 180°) around the axis (axis 2) going through the right and left side.

c) Does the permutation $(1, 2)(3, 4)(5, 6)$ correspond to a symmetry of the cube? Why (not)?

37) a) Let $y = (a_1, \ldots, a_k)$ be a $k$-cycle, and $\sigma$ a permutation. Show that $\sigma^{-1}c\sigma = (\sigma(a_1), \ldots, \sigma(a_k))$.

b) Let $\sigma, \pi \in S_n$. Show that for any $k$ the product $\sigma^{-1}\pi\sigma$ has exactly the same number of $k$-cycles, as $\pi$ has.

c) The German “Enigma” encryption machine, used in the second world war, produced (by a set of moving rotors) in each step a permutation $\sigma \in S_{26}$ (Interpreting the numbers 1-26 as letters in the alphabet.) Show that it is not always possible to use the same setting (i.e. the same permutation $\sigma$) to encrypt and decrypt.

d) To ease handling for the operators (who understood little math), the German military had the “clever” idea to add a “plug-board” (on the picture in front of the machine) that swapped pairs of letters (this creates a permutation $\pi$ that has a cycle type as $(1, 2)(3, 4)(5, 6)\cdots(25, 26)$) and to feed the encryption through the old mechanism ($\sigma$), then through the plug-board, and in reverse back through the mechanism. Show that this encryption is self-reverting, i.e. that $\mu = \sigma^{-1}\pi\sigma$.

e) How many possible $\sigma$ exist. How many possible $\mu$ exists? Explain, based on this count, why consequentially the “clever” idea was really stupid (and indeed was one of the reasons the code could be broken).

Problems marked with a * are bonus problems for extra credit.