Additional Exercises

1. Suppose that p and q are relatively prime positive integers. Show that if $\cos p\alpha$, $\cos q\alpha$, and $\cos(p+q)\alpha$ are all rational, then $\cos\alpha$ is rational.

***2.** Suppose that p and q are relatively prime positive integers. Show that if $\cos p\alpha$ and $\cos q\alpha$ are rational, then $\cos\alpha$ is rational or α is a multiple of $\pi/6$.

3. Suppose we extend the definition of divisibility as follows: Let m be a non-zero integer, and let a/b be a rational number in lowest terms, i.e., $(a,b)=1$. We say that m divides a/b, and write $m|a/b$, if $(m,b)=1$ and $m|a$. Suppose also that for rational numbers r, s with denominators relatively prime to m, we say that $r\equiv s \pmod m$ if $m|(r-s)$.
(a) Let r, R, s, S be rational numbers whose denominators are relatively prime to m. Show that if $r\equiv R \pmod m$ and $s\equiv S \pmod m$, then $r+s\equiv R+S \pmod m$ and $rs\equiv RS \pmod m$.
(b) Suppose that $r=a/b$ is a rational number with $(b,m)=1$. Choose an integer $\overline{b}$ such that $b\overline{b}\equiv 1 \pmod m$. Show that $r\equiv a\overline{b} \pmod m$. Show that if c is an integer such that $r\equiv c \pmod m$, then $c\equiv a\overline{b} \pmod m$.
(c) Suppose that a, A, b, B are integers such that $a\equiv A \pmod m$, $b\equiv B \pmod m$, and $(b,m)=1$. Show that $a/b\equiv A/B \pmod m$.

4. Let $f(z)=\sum_{i=0}^{\infty} a_i z^i$ and $g(z)=\sum_{i=0}^{\infty} b_i z^i$ be two formal power series with integral coefficients. (By "formal" we mean that we don't care whether the radius of convergence is positive.) Define $f\equiv g \pmod m$ if $a_i\equiv b_i \pmod m$ for all $i=0,1,\ldots$.
(a) Suppose that f, F, g, G are power series with integral coefficients. Show that if $f\equiv F \pmod m$ and $g\equiv G \pmod m$, then $f+g\equiv F+G \pmod m$ and $fg\equiv FG \pmod m$.
(b) Suppose that f and F are power series with integral coefficients, both of which have constant term 0. Show that if $f\equiv F \pmod m$, then

$$\frac{1}{1+f}\equiv\frac{1}{1+F} \pmod m.$$

5. Let A be an $n\times n$ matrix with integral elements. Show that if $(\det(A),m)=1$, then for any $(c_1,c_2,\ldots,c_n)\in\mathbf{Z}^n$ there is a unique n-tuple $(x_1,x_2,\ldots,x_n)$ of residue classes $\pmod m$ such that

$$(*)\qquad \sum_{j=1}^{n} a_{ij}x_j\equiv c_j \pmod m$$

for $i=1,2,\ldots,n$. Also, show conversely that if $(\det(A),m)>1$, then the number of solutions of $(*)$ is either 0 or >1, depending on the choice of $(c_1,c_2,\ldots,c_n)$.

Additional exercises

6. We recall that the binomial coefficient $\binom{x}{k}$ is a polynomail in x, namely $\binom{x}{k} = x(x-1)\cdots(x-k+1)/k!$. Thus $\binom{-1/3}{k}$ is a rational number, say

$$\binom{-1/3}{k} = \frac{a_k}{q_k}$$

where $(a_k, q_k) = 1$ and $q_k > 0$.
(a) Show that q_k is a power of 3.
(b) Show that a_k is odd if and only if k can be written as a sum of distinct powers of 4.

7. (Nicol–Selfridge) Show that if n is an odd integer > 3, then there is a prime number p such that $p \nmid n$ and $p|(2^{\varphi(n)} - 1)$.