MA2215: Fields, rings, and modules
Homework problems due on November 19, 2012

1. Clearly, it is enough to check it for $f(x) = x^k$, since every polynomial is a linear combination of these, and if $x - a$ divides each of the summands, it divides the whole sum too. But $x^k - a^k = (x - a)(x^{k-1} + x^{k-2}a + \ldots + xa^{k-2} + a^{k-1})$. The statement about the roots is clear: $f(x) = q(x)(x - a) + f(a)$, so if $f(a) = 0$, then $f(x) = q(x)(x - a)$. The other way round, $f(x) = q(x)(x - a)$, we substitute $x = a$ and conclude $f(a) = 0$.

2. (**a**) Taking common factors out, we may assume that $c(f) = 1$. By previous question, $x-\frac{p}{q}$ divides $f(x)$ in $\mathbb{Q}[x]$. In $\mathbb{Q}[x]$, we can also say that $qx-p$ divides $f(x)$. As proved in class, this implies that $qx - p$ divides $f(x)$ in $\mathbb{Z}[x]$. Comparing the leading terms and the constant terms, we conclude that indeed p is a divisor of the constant term of this polynomial, and q is a divisor of its leading coefficient.

(**b**) This generalisation is trivial: the argument only uses Gauss lemma which is true in that generality.

3. (**a**) Let us prove by induction on n that there exist a polynomial $f_n(x) \in \mathbb{Z}[x]$ of degree n with the leading coefficient 2^{n-1} and a polynomial $g_n(x) \in \mathbb{Z}[x]$ of degree $n-1$ with the leading coefficient 2^{n-1} for which $\cos(n\alpha) = f_n(\cos\alpha)$ and $\sin(n\alpha) = \sin\alpha g_n(\cos\alpha)$. For $n = 1$ we take $f_1(x) = x$ and $g_1(x) = 1$, and the statement is trivial. Let us assume that we know this statement for some n. Since $\cos((n+1)\alpha) = \cos(n\alpha+\alpha) = \cos(n\alpha)\cos\alpha - \sin(n\alpha)\sin\alpha$, we have $\cos((n+1)\alpha) = f_n(\cos\alpha)\cos\alpha - g_n(\cos\alpha)\sin^2\alpha = f_n(\cos\alpha)\cos\alpha - g_n(\cos\alpha)(1-\cos^2\alpha)$, and we can put $f_{n+1}(x) = xf_n(x) - g_n(x)(1 - x^2)$, which is a polynomial of degree $n + 1$ in $\cos\alpha$ with the leading coefficient 2^n. Similarly, since

$$\sin((n+1)\alpha) = \sin(n\alpha+\alpha) = \sin(n\alpha)\cos\alpha + \sin(n\alpha)\cos\alpha,$$

we have

$$\sin((n+1)\alpha) = g_n(\cos\alpha)\sin\alpha\cos\alpha + f_n(\cos\alpha)\sin\alpha = \sin\alpha(g_n(\cos\alpha)\cos\alpha + f_n(\cos\alpha)),$$

and we can put $g_{n+1}(x) = xg_n(x) + f_n(x)$, which is a polynomial of degree n with the leading coefficient 2^n.

(**b**) If $\arccos\frac{3}{5} = \frac{k}{l}\pi$, we have $\cos(2l\arccos\frac{3}{5}) = 1$, so $3/5$ is a root of the polynomial with integer coefficients and the leading coefficient 2^{2l-1}, which contradicts the second question from this sheet.

4. The Eisenstein criterion applies with $p = 3$.

5. If $x^{105} - 9 = g(x)h(x)$ in $\mathbb{Z}[x]$, then some of the complex roots of $x^{105} - 9$ are roots of $g(x)$, and others are roots of $h(x)$. The constant term of $g(x)$ is the product of those roots, and its absolute value is the product of absolute values, which are all equal to $\sqrt[105]{9}$. Clearly, the smallest power of that number that is an integer is 105, so $g(x)$ cannot be both of smaller degree and have integer coefficients.

6. (**a**) Because of the second question of this problem sheet, integer roots of $f(x)$ can only be ±1 and $\pm p$. Moreover, 1 and p are not roots since all the coefficients are positive, -1 is not a root since $f(-1) = \frac{p-1}{2}$ by direct inspection, and p is not a root, since $f(p) \equiv p + p(p-1) + p^2(p-2) \equiv -p^2 \pmod{p^3}$.

(**b**) Indeed,

$$(x-1)f(x) = x^p + 2x^{p-1} + 3x^{p-2} + \ldots + (p-1)x^2 + px - x^{p-1} - 2x^{p-2} - 3x^{p-3} + \ldots - (p-1)x - p$$

which is equal to $x^p + x^{p-1} + \ldots + x - p$, and $(x-1)^2 f(x) = x^{p+1} - (p+1)x + p$.

(**c**) Considering $f(x+1)$ modulo p, we obtain

$$\frac{(x+1)^{p+1} - (p+1)(x+1) + p}{x^2} = \sum_{k=2}^{p+1} \binom{p+1}{k} x^{k-2} \equiv x^{p+1} + x^p \pmod{p},$$

since $\binom{p+1}{k} = \frac{(p+1)!}{k!(p+1-k)!}$, which is divisible by p unless $k = 0, 1, p, p+1$. The terms with $k = 0, 1$ are missing anyway, and the terms with $k = p, p+1$ give x^p and x^{p+1} respectively. If $f(x) = g(x)h(x)$, we have $f(x+1) = g(x+1)h(x+1)$, and modulo p we have $x^{p+1} + x^p = g_1(x)h_1(x)$, where $g_1(x)$ and $h_1(x)$ are the modulo p representatives of $g(x+1)$ and $h(x+1)$. Since the constant term of $f(x+1)$ is $\binom{p+1}{2} = \frac{p(p+1)}{2}$, it is not divisible by p^2, so one of the constant terms of $g_1(x)$ and $h_1(x)$ is not equal to zero. The respective polynomial then must be of degree 1, since the product $g_1(x)h_1(x)$ has all roots but one equal to zero. Finally, we know that our polynomial has no integer roots, so it cannot have factors of degree 1.