MATH7421 Solutions Week 1

Solving Integer Problems using Commutative Rings

1. (a) Suppose that $x, y \in \mathbb{Z}$ satisfy $x^3 - y^2 = 1$. Then we may rearrange and factor as follows:

$$x^3 = 1 + y^2 = (1 + iy)(1 - iy).$$

We claim that the two brackets are coprime in $\mathbb{Z}[i]$. Suppose that $\pi \in \mathbb{Z}[i]$ is irreducible and satisfies $\pi|(1 + yi)$ and $\pi|(1 - yi)$. Then $\pi|(1 + yi) + (1 - yi) = 2$. Taking absolute values shows that $|\pi|^2$ divides 4, so that $|\pi|^2 = 1, 2, 4$. We cannot have that $|\pi|^2 = 1$, since then $\pi = \pm 1, \pm i$ (all of which are units so aren't irreducible). Hence $|\pi|^2 = 2$ or 4. However, $|\pi|^2$ also divides $|(1 + yi)|^2 = 1 + y^2$, so that $1 + y^2 \equiv 0 \bmod 2$. This implies that y is odd. This gives a contradiction since then we have that $x^3 \equiv y^2 + 1 \equiv 2 \bmod 4$ and we can check that 2 is not a cube mod 4.

Since $(1 + yi)$ and $(1 - iy)$ are coprime and their product is a cube then by unique factorisation each is a unit multiplied by a cube. Since the units are $\{1, -1, i, -i\}$ and each is a cube of another unit, we may assume that $(1 + yi) = (a + bi)^3$ is a cube. Then:

$$1 + yi = (a + bi)^3 = (a^3 - 3ab^2) + (3a^2b - b^3)i = a(a^2 - 3b^2) + b(3a^2 - b^2)i.$$

In particular we would have that $a(a^2 - 3b^2) = 1$ and since this is an equality of integers we have that $a = \pm 1$. If $a = -1$ then we have that $1 - 3b^2 = -1$, so that $3b^2 = 2$, which has no integer solution.

Hence $a = 1$ and $1 - 3b^2 = 1$, giving $b = 0$. This gives $y = b(3a^2 - b^2) = 0$ and $x = 1$. This shows that the only integer solution is $(x, y) = (1, 0)$.

(b) Yes! We have that $2^3 + 1 = 8 + 1 = 9 = 3^2$. This is the only solution, as first proved by Lebesgue in 1850. The famous Catalan Conjecture (proved by Preda Mihăilescu in 2002) shows that in fact 8 and 9 are the only consecutive positive perfect powers.

2. (a) Suppose that $\pi \in \mathbb{Z}[i]$ is irreducible and satisfies $\pi|(x + iy)$ and $\pi|(x - iy)$. Then $\pi|(x + iy) + (x - iy) = 2x$, so that $\pi|2$ or $\pi|x$.

- If $\pi|x$ then $\pi|(x + iy) - x = iy$ and so $\pi|y$ (since i is a unit). Since $x^2 + y^2 = z^2$ this also implies that $\pi|z$. It follows that $|\pi|^2 \in \mathbb{Z}$ divides all of x^2, y^2 and z^2. Thus any prime p dividing $|\pi|^2$ would also divide all of x^2, y^2 and z^2, hence would divide all of x, y and z, contradicting the fact that $\gcd(x, y, z) = 1$. There must exist such a prime since $|\pi|^2 > 1$ (the only solutions to $|x + iy|^2 = x^2 + y^2 = 1$ are $(x, y) = (\pm 1, 0), (0, \pm 1)$, which correspond to the units $\pm 1, \pm i \in \mathbb{Z}[i]$).

- If $\pi|2$ then $|\pi|^2$ divides 4. Again, $|\pi|^2 \neq 1$, so that $|\pi|^2 = 2$ or 4. Since $\pi|(x+iy)$, we would have that $2|x^2+y^2 = z^2$, so that $2|z$, hence that $4|z^2$. This would mean that $x^2+y^2 \equiv z^2 \equiv 0 \bmod 4$, and the only solution to this congruence is $x \equiv y \equiv 0 \bmod 2$. Thus all of x, y, z would be even, contradicting the fact that $\gcd(x, y, z) = 1$.

It follows that $(x + iy)$ and $(x - iy)$ are coprime in $\mathbb{Z}[i]$.

(b) Since k, s, t are integers satisfying $k > 0$ and $s > t > 0$ we see that the triple of integers $(x, y, z) = (k(s^2 - t^2), 2st, k(s^2 + t^2))$ are all positive, as required.

It is now a simple computation to check that these numbers satisfy:

$$\begin{aligned} x^2 + y^2 &= (k(s^2 - t^2))^2 + (2st)^2 \\ &= k^2((s^2 - t^2) + 4s^2t^2) \\ &= k^2(s^4 + 2s^2t^2 + t^4) \\ &= k^2(s^2 + t^2)^2 \\ &= (k(s^2 + t^2))^2 \\ &= z^2 \end{aligned}$$

3. (a) We're interested in $(p-1)! \equiv 1 \cdot 2 \cdot 3 \cdot ... \cdot (p-1) \mod p$. Each integer $1 \leq a \leq p-1$ has a unique multiplicative inverse mod p, i.e. $1 \leq b \leq (p-1)$ such that $ab \equiv 1 \bmod p$. Note that if $b \equiv a^{-1} \bmod p$ then $a \equiv b^{-1} \bmod p$, so that every such number is either part of an inverse pair or is self-inverse.

If (a, b) are an inverse pair mod p, then we can cancel both a and b from the factorial mod p, so that:

$$(p-1)! \equiv \prod_{a^2 \equiv 1 \bmod p} a.$$

The self inverse elements satisfy $a^2 \equiv 1 \bmod p$, i.e. $(a-1)(a+1) \equiv 0 \bmod p$. Since p is prime, it follows that $a \equiv \pm 1 \bmod p$, so that the only self-inverse elements are $a = 1$ and $a = (p-1)$. Hence $(p-1)! \equiv 1 \cdot (p-1) \equiv p - 1 \equiv -1 \bmod p$.

(b) Let $x = \left(\frac{p-1}{2}\right)!$. Then (noting that $(-1)^{\frac{p+1}{2}} = -1$ since $p \equiv 1 \bmod 4$):

$$\begin{aligned} x^2 &= \left(1 \cdot 2 \cdot 3... \cdot \left(\frac{p-1}{2}\right)\right)\left(1 \cdot 2 \cdot 3... \cdot \left(\frac{p-1}{2}\right)\right) \\ &\equiv (-1)^{\frac{p-1}{2}} \left(1 \cdot 2 \cdot 3... \cdot \left(\frac{p-1}{2}\right)\right)\left((-1) \cdot (-2) \cdot (-3)... \cdot - \left(\frac{p-1}{2}\right)\right) \\ &\equiv (-1)^{\frac{p-1}{2}} \left(1 \cdot 2 \cdot 3... \cdot \left(\frac{p-1}{2}\right)\right)\left((p-1) \cdot (p-2) \cdot (p-3)... \cdot \left(\frac{p+1}{2}\right)\right) \\ &\equiv (-1)^{\frac{p-1}{2}}(p-1)! \\ &\equiv (-1)^{\frac{p+1}{2}} \\ &\equiv -1 \bmod p \end{aligned}$$

4. (a) Suppose that $n = x^2 + y^2$ is a sum of two squares and has a prime divisor that satisfies $p \equiv 3 \bmod 4$. Then p is irreducible in $\mathbb{Z}[i]$ and divides $n = (x + iy)(x - iy)$, so that $p|(x + iy)$ or $p|(x - iy)$. In either case we would have $(x \pm iy) = p(z + iw)$ for some $z, w \in \mathbb{Z}$, so that $p|x$ and $p|y$. This implies that $p^2|n$ (alternatively, taking absolute values gives $p^2|x^2 + y^2 = n$).

(b) We use strong induction on n. First note that the result is true for the base case $n = 1$ (since $1 = 1^2 + 0^2$ is a sum of two squares and **every** prime dividing n does so to an even power, namely 0).

Assume that the result is known for all $1 \leq m \leq n-1$ and we aim to prove the result for n. Suppose that $n = x^2 + y^2$ is a sum of two squares:

- If there are **no** primes $p|n$ with $p \equiv 3 \bmod 4$ then we are done (since then every such prime will automatically divide n to an even power, namely 0).
- Otherwise there exists **at least one** prime $p|n$ with $p \equiv 3 \bmod 4$. Part (a) then tells us that $p^2|n$, so that $\frac{n}{p^2} = \left(\frac{x}{p}\right)^2 + \left(\frac{y}{p}\right)^2 = x'^2 + y'^2$ for two integers $x', y' \in \mathbb{Z}$. Hence $\frac{n}{p^2}$ is also a sum of two squares.

The inductive hypothesis then tells us that $\frac{n}{p^2} = k$ must have all prime divisors $q \equiv 3 \bmod 4$ dividing to an even power. The same is then true for $n = kp^2$.

(c) Suppose $m = x^2 + y^2$ and $n = z^2 + w^2$ for $x, y, z, w \in \mathbb{Z}$. Then:

$$mn = (x^2 + y^2)(z^2 + w^2) = x^2z^2 + x^2w^2 + y^2z^2 + y^2w^2 = (xz + yw)^2 + (xw - yz)^2.$$

(d) Suppose that every $p|n$ such that $p \equiv 3 \bmod 4$ divides n to an even power. By factoring out the biggest square dividing n we may write n as $n = n_1 n_2^2$ with n_1 square-free.

- If $n_1 = 1$ then $n = n_2^2 = n_2^2 + 0^2$ is a sum of two squares.
- Otherwise, n_1 is a product of primes that are either 2 or 1 mod 4. Since we have already proved that all such primes are a sum of two squares, it follows from part (c) that the product n_1 is a sum of two squares, i.e. $n_1 = x^2 + y^2$ for some $x, y \in \mathbb{Z}$. It now follows that $n = n_2^2(x^2 + y^2) = (xn_2)^2 + (yn_2)^2$ is a sum of two squares.

5. First we will show that a prime p can be written as $p = x^2 + 2y^2$ if and only if p is reducible in $\mathbb{Z}[\sqrt{-2}]$.

If $p = x^2 + 2y^2$ then it would lead to a factorisation $p = (x + y\sqrt{-2})(x - y\sqrt{-2})$ in $\mathbb{Z}[\sqrt{-2}]$. Neither factor can be a unit, since this would imply that $y = 0$, so that $p = x^2$ (since the units of $\mathbb{Z}[\sqrt{-2}]$ are ± 1). Hence, p is reducible in $\mathbb{Z}[\sqrt{-2}]$.

If p is reducible in $\mathbb{Z}[\sqrt{-2}]$ then it admits a decomposition $p = \alpha\beta$ with $\alpha, \beta \in \mathbb{Z}[i]$ non-units. Then taking absolute values gives $p^2 = |\alpha|^2|\beta|^2$, and the only possibility is $|\alpha|^2 = |\beta|^2 = p$. Writing $\alpha = x + y\sqrt{-2}$ gives $p = x^2 + 2y^2$.

It now suffices to understand which primes p are reducible in $\mathbb{Z}[\sqrt{-2}]$. First note that $2 = (\sqrt{-2})^2$ is reducible (and $2 = 0^2 + 2(1)^2$), so we may assume that p is odd. Next note that the squares mod 8 are $0, 1, 4$, and so $x^2 + 2y^2 \equiv 0, 1, 2, 3, 4, 6 \bmod 8$. It follows that if $p \equiv 5, 7 \bmod 8$ then p is irreducible in $\mathbb{Z}[\sqrt{-2}]$ (equivalently, p cannot be written as $p = x^2 + 2y^2$).

If $p \equiv 1, 3 \bmod 8$ then we can find $x \in \mathbb{Z}$ such that $x^2 \equiv -2 \bmod p$ (as given in the question). It follows that $p \mid x^2 + 2 = (x + \sqrt{-2})(x - \sqrt{-2})$. If p is irreducible in $\mathbb{Z}[\sqrt{-2}]$ then $p|(x + \sqrt{-2})$ or $p|(x - \sqrt{-2})$, which is impossible. Thus p must be reducible in $\mathbb{Z}[\sqrt{-2}]$ (hence p can be written as $p = x^2 + 2y^2$). This finishes the proof that $p = x^2 + 2y^2$ if and only if $p = 2$ or $p \equiv 1, 3 \bmod 8$.

6. (a) Note that $x = 1$ works, since $1^2 \equiv -5 \bmod 3$. However, we cannot write $3 = x^2 + 5y^2$ since we would have to have $y = 0$ and $x^2 = 3$, which is impossible.

   (b) We show that 3 is irreducible in the ring $\mathbb{Z}[\sqrt{-5}]$. Suppose that 3 is reducible and that $3 = \alpha\beta$ with $\alpha, \beta \in \mathbb{Z}[\sqrt{-5}]$ non-units. Then taking complex absolute value gives $9 = |\alpha|^2|\beta|^2$, so that $|\alpha|^2 = |\beta|^2 = 3$ (we cannot have either $|\alpha|^2 = 1$ or $|\beta|^2 = 1$, since then one of α, β would be a unit).

   It follows that $3 = |\alpha|^2 = |x + y\sqrt{-5}|^2 = x^2 + 5y^2$, which is impossible.

   (c) We blindly follow the proof in the notes, but adapt to this example. We have that $1^2 \equiv -5 \bmod 3$ implies that $3|1^2 + 5 = (1 + \sqrt{-5})(1 - \sqrt{-5})$ in the ring $\mathbb{Z}[\sqrt{-5}]$.

   We've seen that 3 is irreducible in $\mathbb{Z}[\sqrt{-5}]$, so we are **tempted** to conclude that $3|(1 + \sqrt{-5})$ or $3|(1 - \sqrt{-5})$...but neither of these statements are true, so something must be wrong!

   The problem is that $\mathbb{Z}[\sqrt{-5}]$ does **not** have unique factorisation! We can rewrite the factorisation $(1 + \sqrt{-5})(1 - \sqrt{-5}) = 6 = 3 \cdot 2$ in a completely different way so that the RHS now visibly has a factor divisible by 3!

   In the ring $\mathbb{Z}$, irreducible elements (previously known as primes) also satisfy the prime property, that $p|ab$ implies $p|a$ or $p|b$. However, more general rings like $\mathbb{Z}[\sqrt{-5}]$ can have irreducibles that do not satisfy the prime property. As we will see later, this is intimately linked to the failure of unique factorisation!

7. (a) We know that the solutions to $x^2 - 2y^2 = \pm 1$ are in bijection with units in $\mathbb{Z}[\sqrt{2}]$, which we've given are all of the form $\pm(1 + \sqrt{2})^n$ for some $n \in \mathbb{Z}$.

   Suppose that the unit $(1 + \sqrt{2})^n = x + y\sqrt{2}$ corresponds to the solution (x, y). Then a simple calculation shows that the unit

   $$(1 + \sqrt{2})^{-n} = (-1)^{-n}(1 - \sqrt{2})^n = (-1)^{-n}(x - y\sqrt{2})$$

   corresponds to the solution $(x, -y)$ or $(-x, y)$ (depending on the parity of n). Thus the four units $\pm(1 + \sqrt{2})^n$ and $\pm(1 - \sqrt{2})^{-n}$ give rise to the four solutions $(\pm x, \pm y)$.

   Now we only need study the solutions arising from $(1 + \sqrt{2})^n$ with $n \geq 0$. The first such unit is $(1 + \sqrt{2})^0 = 1$, leading to solution $(a_0, b_0) = (1, 0)$. Now suppose that $(1 + \sqrt{2})^n = (a_n + b_n\sqrt{2})$. Then

   $$(1 + \sqrt{2})^{n+1} = (1 + \sqrt{2})(a_n + b_n\sqrt{2}) = (a_n + 2b_n) + (a_n + b_n)\sqrt{2}.$$

   This tells us that consecutive solutions are related by the recursion

   $$(a_{n+1}, b_{n+1}) = (a_n + 2b_n, a_n + b_n),$$

   as required.

   (b) We recover four positive integer solutions as follows:

   $$\begin{aligned}(a_0, b_0) &= (1, 0)\\ (a_1, b_1) &= (a_0 + 2b_0, a_0 + b_0) = (1, 1)\\ (a_2, b_2) &= (a_1 + 2b_1, a_1 + b_1) = (3, 2)\\ (a_3, b_3) &= (a_2 + 2b_2, a_2 + b_2) = (7, 5)\end{aligned}$$

Polynomials, Roots and Irreducibility

1. (a) Suppose that $a = \frac{b}{c} \in \mathbb{Q}$ is a rational root of $f(x)$ with $\gcd(b, c) = 1$. Then:

$$0 = f\left(\frac{b}{c}\right) = a_0 + a_1\left(\frac{b}{c}\right) + a_2\left(\frac{b}{c}\right)^2 + ... + a_{n-1}\left(\frac{b}{c}\right)^{n-1} + a_n\left(\frac{b}{c}\right)^n.$$

Multiplying both sides by c^n gives:

$$0 = a_0c^n + a_1c^{n-1}b + a_2c^{n-2}b^2 + ... + a_{n-1}cb^{n-1} + a_nb^n.$$

Note that this is an equality of integers (since we assumed that $f(x) \in \mathbb{Z}[x]$, so that $a_i \in \mathbb{Z}$ for all i). Rearranging gives:

$$a_0c^n + a_1c^{n-1}b + ... + a_{n-1}cb^{n-1} = -a_nb^n$$
$$a_1c^{n-1}b + a_2c^{n-2}b^2 + ... + a_{n-1}cb^{n-1} + a_nb^n = -a_0c^n$$

The first equation shows that $c \,|\, -a_nb^n$, whereas the second shows that $b \,|\, -a_0c^n$. Since $\gcd(b, c) = 1$ we must have that $c \,|\, a_n$ and $b \,|\, a_0$, as required

(b) By the Rational Root Test, any rational root $a = \frac{b}{c}$ of $f(x) = x^3 + 3x + 1 \in \mathbb{Z}[x]$ must satisfy $c \,|\, 1$ and $b \,|\, 1$. It follows that $b, c = \pm 1$ and so $a = \pm 1$. Since $f(\pm 1) \neq 0$ we conclude that $f(x)$ has no rational roots.

We can also conclude that $f(x)$ is irreducible over $\mathbb{Q}$, since any non-trivial factorisation $f(x) = g(x)h(x)$ must involve a linear factor (since otherwise we would have $\deg(f(x)) \geq 4$). Such a linear factor cannot exist, since it would correspond to a rational root.

(c) By the Rational Root Test, any rational root $a = \frac{b}{c}$ of $f(x) = x^4 - 4 \in \mathbb{Z}[x]$ must satisfy $c \,|\, 1$ and $b \,|\, -4$. It follows that $c = \pm 1$ and $b = \pm 1, \pm 2, \pm 4$ and so $a = \pm 1, \pm 2, \pm 4$. Since $f(\pm 1) \neq 0$, $f(\pm 2) \neq 0$ and $f(\pm 4) \neq 0$ we conclude that $f(x)$ has no rational roots.

In this case, we find that $f(x)$ is reducible over $\mathbb{Q}$, since we clearly have the factorisation $f(x) = (x^2 - 2)(x^2 + 2)$. This simple example shows that checking a polynomial is irreducible requires more care than just checking it doesn't have a root!

2. Let $\deg(f(x)) = d$. By the rational root test, every rational root $a = \frac{b}{c}$ is such that c divides the coefficient of x^d. However, $f(x)$ is monic and so this coefficient is 1. Hence $c = \pm 1$, so that the root is $a = \pm b \in \mathbb{Z}$.

3. We're given the factorisation $f(x) = g(x)h(x)$ with $g(x), h(x) \in \mathbb{Q}[x]$. By Gauss' Lemma there exists a related factorisation $f(x) = s(x)t(x)$ with $s(x), t(x) \in \mathbb{Z}[x]$. Reading the proof carefully, we see that in fact $s(x), t(x)$ are rational multiples of $g(x), h(x)$ in some order. Swapping if necessary we may suppose that $s(x) = \lambda g(x)$ and $t(x) = \mu h(x)$ for some $\lambda, \mu \in \mathbb{Q}$. (In fact, $\mu = \lambda^{-1}$, but this will not matter).

Now note that since $f(x)$ is monic (by assumption), we find that the leading coefficients of $s(x)$ and $t(x)$ must multiply to 1. However, these coefficients are integers and so they must either both be 1 or both be -1. Swapping $s(x) \mapsto -s(x)$ and $t(x) \mapsto -t(x)$ if necessary then allows us to assume that both $s(x)$ and $t(x)$ are monic without changing the factorisation above.

Since $g(x)$ and $h(x)$ are also monic (by assumption) we must then have that $\lambda = \mu = 1$, so that $g(x) = s(x)$ and $h(x) = t(x)$ are both in $\mathbb{Z}[x]$.

4. (a) This polynomial is irreducible by Eisenstein's Criterion with $p = 7$.

   (b) This polynomial is irreducible by Eisenstein's Criterion with $p = 11$.

5. (a) Suppose that $f(x) \in \mathbb{Q}[x]$ is reducible and that $f(x) = g(x)h(x)$ is a non-trivial factorisation over $\mathbb{Q}$. Then $f(x+a) = g(x+a)h(x+a)$ is a non-trivial factorisation over $\mathbb{Q}$ for any $a \in \mathbb{Q}$ (since the degrees are preserved by this change of variables). It follows that $f(x+a)$ is reducible for every $a \in \mathbb{Q}$.

   Conversely, if $f(x+a) \in \mathbb{Q}[x]$ is reducible for every $a \in \mathbb{Q}$ then taking $a = 0$ shows that $f(x)$ is reducible over $\mathbb{Q}$.

   (b) Making the substitution $x \mapsto x+1$ we get the polynomial:

$$(x+1)^4 + 4(x+1) + 1 = (x^4 + 4x^3 + 6x^2 + 4x + 1) + (4x + 4) + 1 = x^4 + 4x^3 + 6x^2 + 8x + 6.$$

   This polynomial is in $\mathbb{Z}[x]$ and so is irreducible by Eisenstein's Criterion with $p = 2$. Hence the original polynomial is irreducible by the contrapositive of part (a).

6. (a) It's clear that $f_p(1) = 1^p - 1 = 0$, so that $x - 1 \,|\, f_p(x)$. One easily computes that the other factor is $x^{p-1} + x^{p-2} + ... + x + 1$. (Fans of the geometric series formula should notice this factorisation instantly!)

   (b) To see this write $\phi_p(x) = \frac{x^p - 1}{x - 1}$ and make the substitution $x \mapsto x + 1$ to get:

$$\frac{(x+1)^p - 1}{(x+1) - 1} = \frac{(x+1)^p - 1}{x} = \frac{(x^p + \binom{p}{1}x^{p-1} + \binom{p}{2}x^{p-2} + ... + \binom{p}{p-1}x + 1) - 1}{x}$$
$$= x^{p-1} + \binom{p}{1}x^{p-2} + \binom{p}{2}x^{p-3} + ... + \binom{p}{p-1}.$$

   We claim that this polynomial is irreducible by Eisenstein's Criterion with prime p. To prove this, we note that:

   - The leading coefficient is $a_{p-1} = 1$, and $p \nmid 1$.
   - All of the other coefficients are $\binom{p}{i}$ for $1 \leq i \leq p-1$. These are all divisible by p since:
$$\binom{p}{i} = \frac{p!}{i!(p-i)!} \in \mathbb{Z}$$
     and clearly $p \,|\, p!$ but $p \nmid i!(p-i)!$ (since p is prime and p doesn't divide any of the numbers in this product if $1 \leq i \leq p-1$).
   - The constant term is $a_0 = \binom{p}{p-1} = p$ and $p^2 \nmid p$.

   (c) No. If $n = 4$ then we get the polynomial $x^3 + x^2 + x + 1 \in \mathbb{Q}[x]$, which has $x = -1$ as a root, hence is divisible by $x+1$ (giving the factorisation $x^3 + x^2 + x + 1 = (x+1)(x^2+1)$). This makes sense, since the roots of $x^4 - 1$ are $\{\pm 1, \pm i\}$ so that we already expected two linear factors.

   In fact, it is possible to show that the **only** values of n that make this polynomial irreducible are prime.

7. If $f(x)$ has a repeated root $a \in \mathbb{C}$ then $f(x) = (x-a)^m g(x)$ for some $m \geq 2$ and $g(x) \in \mathbb{C}[x]$. You might be tempted at this point to say that this is a non-trivial factorisation of $f(x)$, but it might not be the case that $g(x) \in \mathbb{Q}[x]$, i.e. it might not be a valid factorisation in $\mathbb{Q}[x]$.

   Instead, consider the derivative $f'(x) \in \mathbb{Q}[x]$. This satisfies:

$$f'(x) = m(x-a)^{m-1}g(x) + (x-a)^m g'(x) = (x-a)^{m-1}(mg(x) + (x-a)g'(x)).$$

   It follows that $\gcd(f(x), f'(x))$ is non-constant (both polynomials are divisible by $(x-a)$). This is a contradiction since $f(x)$ is irreducible so that $\gcd(f(x), f'(x))$ is constant (we cannot have that $f(x)|f'(x)$ since $\deg(f'(x)) < \deg(f(x))$.