

Problem 1.

Suppose that  $|\cdot|$  is a valuation on  $\mathbb{Q}(i)$ . Then its restriction to  $\mathbb{Q}$  gives us a valuation on  $\mathbb{Q}$ , and so by Ostrowski's theorem, it is equivalent to either the trivial valuation, the standard absolute value or the  $p$ -adic valuation for some prime  $p$ .

Now, we can extend the trivial valuation on  $\mathbb{Q}$  to the trivial valuation on  $\mathbb{Q}(i)$  (by setting  $|a + bi| = 1$  for all  $a, b \in \mathbb{Q}$ )

Now suppose that this restriction of  $|\cdot|$  to  $\mathbb{Q}$  is (equivalent to) the usual absolute value. Since  $(a + bi)(a - bi) = (a^2 + b^2)$  and since  $|\cdot|$  has the property  $|xy| = |x||y|$  for all  $x, y$ , we see that  $|a + bi||a - bi| = |a^2 + b^2|_\infty$  where  $|\cdot|_\infty$  denotes the usual absolute value. So we can define  $|a + bi| = \sqrt{a^2 + b^2}$ . (it is not hard to check that this satisfies all the properties of a valuation. The triangle inequality follows from the fact that for any two complex numbers  $z$  and  $w$ ,  $|z + w| \leq |z| + |w|$ )

Finally, suppose that the restriction is a  $p$ -adic valuation for some prime  $p$ . Since any element of  $\mathbb{Q}(i)$  can be written as a quotient of two elements of  $\mathbb{Z}[i]$ , we just need to define  $|a + bi|$  where  $a, b \in \mathbb{Z}$ . Note that for any integer  $n$ ,  $|n| \leq 1$  and so by triangle inequality  $|a + bi| \leq |a| + |b| \leq 2$ . In fact, note that we must have  $|a + bi| \leq 1$  (if  $|a + bi| > 1$  for some integers  $a, b$ , then we can raise  $|a + bi|$  to some huge power, and we'd get that  $|a + bi|^k > 2$  for some large  $k$ . Now, since  $\mathbb{Z}[i]$  is Euclidean, it has the unique factorization property, and hence it suffices to extend the  $p$ -adic valuation to the primes of  $\mathbb{Z}[i]$ . Now, recall that the prime integers that are congruent to  $3 \pmod{4}$  remain primes in  $\mathbb{Z}[i]$ , so we just need to extend the  $p$ -adic valuation to  $1 + i$  and the primes of  $\mathbb{Z}[i]$  that divide integer primes congruent to  $1 \pmod{4}$ .

Suppose first  $p = 2$ . Then, since  $2 = -i(1 + i)^2$ , we see that  $|1 + i|^2 = (1/2)$ , so we must define  $|1 + i| = (1/\sqrt{2})$ . Also, if  $\pi$  is a prime such that  $\pi\bar{\pi} = q$  where  $q$  is an integer prime congruent to  $1 \pmod{4}$ , then  $|\pi||\bar{\pi}| = 1$  and thus we must have  $|\pi| = |\bar{\pi}| = 1$ .

Now, if  $p$  is odd then the valuation of any prime of  $\mathbb{Z}[i]$  that does not divide  $p$  will be equal to 1 (this is similar to the computation above), so we just need to determine what happens with the primes that do divide  $p$ . Write  $\pi\bar{\pi} = p$  and so  $|\pi||\bar{\pi}| = (1/p)$ . Note that  $\pi$  and  $\bar{\pi}$  are coprime and in fact, any powers of  $\pi$  and  $\bar{\pi}$  are coprime. This means that we canNOT have both  $|\pi| < 1$  and  $|\bar{\pi}| < 1$ . Indeed, for any integer  $k$  we may write  $1 = a\pi^k + b\bar{\pi}^k$  for some constants  $a$  and  $b$  (of course, these constants depend on  $k$ ). Then the triangle inequality implies that  $1 \leq |a||\pi|^k + |b||\bar{\pi}|^k$ , so if both  $|\pi| < 1$  and  $|\bar{\pi}| < 1$  then by letting  $k$  tends to infinity we'd get a contradiction (because then  $|a||\pi|^k$  and  $|b||\bar{\pi}|^k$  would tend to 0, and so their sum would not be greater than 1)

Hence we see that exactly one of  $|\pi|$  or  $|\bar{\pi}|$  is going to be equal to 1 while the other one will be equal to  $1/p$ . (So there are two extensions of the  $p$ -adic valuation in this case. In the first one  $|\pi| = 1$  and  $|\bar{\pi}| = (1/p)$  while in the second one  $|\bar{\pi}| = 1$  and  $|\pi| = (1/p)$ .)

Problems 2 and 3.

Let's begin by showing that this ring is Euclidean. So we need to show that given  $x, y \in \mathbb{Z}[\sqrt{-2}]$  and  $y \neq 0$  there exist  $q, r$  in this ring such that  $x = qy + r$ , and either  $r = 0$  or  $N(r) < N(y)$  where  $N$  is the norm map ( $N(a + b\sqrt{-2}) = a^2 + 2b^2$ )

To do this, we observe that  $x/y$  can be written in the form  $u + v\sqrt{-2}$  where  $u, v$  are rational numbers (indeed, if  $x = a + b\sqrt{-2}$  and  $y = c + d\sqrt{-2}$  then  $u = (ac + 2bd)/(c^2 + 2d^2)$  and  $v = (bc - ad)/(c^2 + 2d^2)$ .)

Now choose integers  $s$  and  $t$  such that  $|u - s| \leq 1/2$  and  $|v - t| \leq 1/2$  ( $s$  and  $t$  are the nearest integers for  $u$  and  $v$  respectively). Define  $q = s + t\sqrt{-2}$  and  $r = x - qy$  so that  $x = qy + r$ . If  $r = 0$ , we're done, so assume that  $r \neq 0$ . We must show that  $N(r) < N(y)$ , equivalently  $N(r/y) < 1$ . Now,  $r/y = (x/y) - q = (u - s) + (v - t)\sqrt{-2}$  and so  $N(r/y) = (u - s)^2 + 2(v - t)^2 \leq (1/2)^2 + 2 \cdot (1/2)^2 = 3/4 < 1$ . Thus,  $N(r/y) < 1$ , and so we are done.

Let us now explain why the unique factorization holds. Since this ring is Euclidean, we know that the division algorithm holds. Hence the Euclidean algorithm holds (and as we know, this algorithm allows us to express the gcd of two elements as a linear combination of these elements.) Next, recall that the key fact in the proof of the unique factorization of integers was that if a prime  $p$  divides the product  $ab$  then either  $p$  divides  $a$  or  $p$  divides  $b$ . We'll show that the same property

holds for the ring  $\mathbb{Z}[\sqrt{-2}]$ . So suppose that a prime  $p$  divides  $ab$  where  $p, a, b$  are elements of  $\mathbb{Z}[\sqrt{-2}]$ . If  $p$  divides  $a$ , we're done, so assume that it does not. Since  $p$  is prime, its only divisors are 1 and  $p$  (up to multiplication by a unit), and so since  $p$  does not divide  $a$ , it follows that the gcd of  $a$  and  $p$  is 1. By Euclidean algorithm we may write  $1 = xp + ya$  for some  $x, y$  in  $\mathbb{Z}[\sqrt{-2}]$ . Then  $b = xpb + yab$ .  $p$  clearly divides both  $xpb$  and  $yab$ , so it follows that  $p$  divides  $b$ . In fact, this argument shows that any Euclidean ring has the unique factorization property.

Next, let's determine the primes of  $\mathbb{Z}[\sqrt{-2}]$ . We begin by making a few observations. First, if  $\pi$  is a prime of  $\mathbb{Z}[\sqrt{-2}]$  then  $\pi \cdot \bar{\pi} = N(\pi)$ , so that there are positive integers which are divisible by  $\pi$ . Let  $n$  be the least positive integer which is divisible by  $\pi$ . I claim that  $n$  must be prime; if  $n = n_1 n_2$ , then since  $\mathbb{Z}[\sqrt{-2}]$  has the unique factorization property, we see that  $\pi | n_1 n_2$  implies that either  $\pi$  divides  $n_1$  or it divides  $n_2$ . Since  $n$  is the least positive integer which is divisible by  $\pi$ , it follows that either  $n_1 = n$  or  $n_2 = n$ , so that  $n$  is prime. Finally, note that if  $\pi$  divided two primes,  $m$  and  $n$  then it would any linear combination of  $m$  and  $n$ . In particular, since we can write  $am + bn = 1$  for some integers  $a$  and  $b$  it follows that  $\pi$  divides 1, which is absurd.

So we conclude that any prime of  $\mathbb{Z}[\sqrt{-2}]$  is a divisor of exactly one positive prime integer. next, let's determine elements of  $\mathbb{Z}[\sqrt{-2}]$  whose norm is 1. If  $a + b\sqrt{-2}$  has norm 1, then  $a^2 + 2b^2 = 1$ . This means that  $b = 0$  (otherwise,  $2b^2 \geq 2$  and so  $a^2 + 2b^2 \geq 2$ ) and then  $a^2 = 1$  so  $a = \pm 1$ . So the only elements of norm 1 in  $\mathbb{Z}[\sqrt{-2}]$  are  $\pm 1$ .

So let's determine how prime integers factor in  $\mathbb{Z}[\sqrt{-2}]$ . Suppose that  $\pi = a + b\sqrt{-2}$  divides a prime integer  $p$ , so we can write  $\pi\gamma = p$  for some  $\gamma \in \mathbb{Z}[\sqrt{-2}]$ . Taking norms gives us  $p^2 = N(\pi)N(\gamma)$ . Since  $\pi$  is prime,  $N(\pi) \neq 1$  and so we see that either  $N(\gamma) = 1$  (which means that  $\gamma = \pm 1$  and thus  $\pi = \pm p$ ) or  $N(\pi) = N(\gamma) = p$ . So we see that a prime integer  $p$  either remains prime in  $\mathbb{Z}[\sqrt{-2}]$  or it is the norm of some prime element  $\pi$ . In this case we see that  $p = N(\pi) = a^2 + 2b^2$ . So we need to determine which primes can be written in this form. Since  $2 = 0 + 2 \cdot 1$  we see that 2 is the norm of  $\sqrt{-2}$ , and that  $\sqrt{-2}$  is a prime element of  $\mathbb{Z}[\sqrt{-2}]$ . So from now on let's assume that  $p$  is odd.

Suppose we can write  $p = a^2 + 2b^2$ . Note that neither  $a$  nor  $b$  can be 0 (since no prime number is a square of an integer or twice a square of an integer). Moreover,  $p$  doesn't divide  $a$  and it doesn't divide  $b$  (if  $p$  divided either  $a$  or  $b$  then  $a^2 + 2b^2 \geq p^2 > p$ , a contradiction).

So we have  $a^2 + 2b^2 \equiv 0 \pmod{p}$ . Let  $b'$  be an integer such that  $bb' \equiv 1 \pmod{p}$ . Then  $a^2 \equiv -2b^2 \pmod{p}$ , or  $(ab')^2 \equiv -2 \pmod{p}$ . So we see that if  $p$  can be written in the form  $a^2 + 2b^2$  then  $-2$  is a square mod  $p$ . Since  $\left(\frac{-2}{p}\right) = \left(\frac{-1}{p}\right) \cdot \left(\frac{2}{p}\right)$  we see that  $-2$  is a square mod  $p$  if and only if either  $-1$  and 2 are both quadratic residues mod  $p$  or they both are quadratic nonresidues mod  $p$ . Let's analyze these two cases.

If  $-1$  is a quadratic residue mod  $p$  then we know that  $p \equiv 1 \pmod{4}$ . If 2 is a quadratic residue mod  $p$  then we know that  $p \equiv 1$  or  $7 \pmod{8}$ . Now,  $p \equiv 7 \pmod{8}$  implies  $p \equiv 7 \pmod{4}$  i.e.  $p \equiv 3 \pmod{4}$ . Thus, it is impossible for a prime to be simultaneously congruent to 1 mod 4 and to 7 mod 8. On the other hand,  $p \equiv 1 \pmod{4}$  and  $p \equiv 1 \pmod{8}$  imply that  $p \equiv 1 \pmod{8}$ . Conclusion :  $-1$  and 2 are both quadratic residues mod  $p$  only if  $p \equiv 1 \pmod{8}$ .

If  $-1$  is a quadratic nonresidue mod  $p$  then we know that  $p \equiv 3 \pmod{4}$ . If 2 is a quadratic nonresidue mod  $p$  then we know that  $p \equiv 3$  or  $5 \pmod{8}$ . Now,  $p \equiv 5 \pmod{8}$  implies  $p \equiv 5 \pmod{4}$  i.e.  $p \equiv 1 \pmod{4}$ . Thus, it is impossible for a prime to be simultaneously congruent to 3 mod 4 and to 5 mod 8. On the other hand,  $p \equiv 3 \pmod{4}$  and  $p \equiv 3 \pmod{8}$  imply that  $p \equiv 3 \pmod{8}$ . Conclusion :  $-1$  and 2 are both quadratic residues mod  $p$  only if  $p \equiv 3 \pmod{8}$ .

So  $-2$  is a square mod  $p$  if and only if  $p \equiv 1$  or  $3 \pmod{8}$ . Thus, we can immediately conclude that if  $p \equiv 5$  or  $7 \pmod{8}$  then  $p$  remains prime in  $\mathbb{Z}[\sqrt{-2}]$ .

Now suppose that  $p \equiv 1$  or  $3 \pmod{8}$ . Then, as we just saw,  $-2$  is a square mod  $p$ , so there is an integer  $c$  such that  $c^2 \equiv -2 \pmod{p}$ . This means that  $p$  divides  $c^2 + 2 = (c + \sqrt{-2})(c - \sqrt{-2})$ . If  $p$  remained prime in  $\mathbb{Z}[\sqrt{-2}]$ , then  $p$  would divide either  $(c + \sqrt{-2})$  or  $(c - \sqrt{-2})$ . However,  $(c \pm \sqrt{-2})/p$  does not belong to  $\mathbb{Z}[\sqrt{-2}]$  (the coefficient of  $\sqrt{-2}$  is  $(1/p)$  which is not an integer) and so  $p$  does not remain prime in  $\mathbb{Z}[\sqrt{-2}]$ . So  $p$  can be factored as  $\alpha\beta$  where neither  $\alpha$  nor  $\beta$  is a unit (i.e., neither one of them has norm 1), and so  $p^2 = N(\alpha)N(\beta)$  so that  $p = N(\alpha)$  and if we

write  $\alpha = x + y\sqrt{-2}$  we get that  $p = x^2 + 2y^2$ . So if  $p \equiv 1$  or  $3 \pmod{8}$  then there exist integers  $x, y$  such that  $p = x^2 + 2y^2$ .

So now let's write down what we have gotten so far. The prime elements of  $\mathbb{Z}[\sqrt{-2}]$  are (up to multiplication by a unit, that is, up to multiplication by  $-1$ )

- i)  $\sqrt{-2}$
- ii) Integer primes that are congruent to 5 or 7 mod 8
- iii) the factors  $a \pm b\sqrt{-2}$  of the prime integers that are congruent to either 1 or 3 mod 8.

We also showed that a prime integer  $p$  can be written in the form  $x^2 + 2y^2$  for  $x, y \in \mathbb{Z}$  if and only if  $p = 2$  or  $p$  is congruent to 1 or 3 mod 8.

Finally, let's determine what integers  $n$  can be written as  $x^2 + 2y^2$ . Note that  $n = x^2 + 2y^2 = N(x + y\sqrt{-2})$ . We can factor  $x + y\sqrt{-2}$  into primes of  $\mathbb{Z}[\sqrt{-2}]$ :

$x + y\sqrt{-2} = (\sqrt{-2})^a (\pi_1)^{a_1} (\pi_2)^{a_2} \dots (\pi_r)^{a_r} (q_1)^{b_1} (q_2)^{b_2} \dots (q_s)^{b_s}$  where  $\pi_i$  are the factors of the prime integers that are congruent to either 1 or 3 mod 8 and  $q_j$  are the integer primes that are congruent to either 5 or 7 mod 8. Then

$$N(x + y\sqrt{-2}) = (2^a) (N(\pi_1)^{a_1} (N(\pi_2)^{a_2} \dots (N(\pi_r)^{a_r} (q_1)^{2b_1} (q_2)^{2b_2} \dots (q_s)^{2b_s})$$

Note that  $N(\pi_i)$  are odd primes that are congruent to either 1 or 3 mod 8. So we see that in the prime factorization of  $n$  the exponents of odd prime factors that are congruent to either 5 or 7 mod 8 are even.

Conversely, suppose we're given a number  $n$  such that in the prime factorization of  $n$  the exponents of odd prime factors that are congruent to 5 or 7 mod 8 are all even. I claim that  $n$  can be expressed as  $x^2 + 2y^2$ . Write  $n = 2^a (p_1)^{a_1} \dots (p_r)^{a_r} (q_1)^{2b_1} \dots (q_s)^{2b_s}$  where the  $p_i$  are odd primes that are congruent to either 1 or 3 mod 8 and  $q_j$  are odd primes that are congruent to either 5 or 7 mod 8. Let  $\pi_i$  be a prime element of  $\mathbb{Z}[\sqrt{-2}]$  such that  $\pi_i | p_i$  for all  $i$ . Define  $x + y\sqrt{-2} = (\sqrt{-2})^a (\pi_1)^{a_1} (\pi_2)^{a_2} \dots (\pi_r)^{a_r} (q_1)^{b_1} (q_2)^{b_2} \dots (q_s)^{b_s}$ . Then we see that  $N(x + y\sqrt{-2}) = n$  so that  $x^2 + 2y^2 = n$  as was to be shown. Conclusion: a positive integer  $n$  can be written in the form  $x^2 + 2y^2$  if and only if in the prime factorization of  $n$  the exponents of odd prime factors that are congruent to either 5 or 7 mod 8 are all even.

Problem 4.

Note that if  $(x, y, z)$  is a solution to this equation, and  $d$  is the gcd of  $x, y$  and  $z$ , then  $(x/d, y/d, z/d)$  also solves this equation, and now the gcd of  $x/d, y/d$  and  $z/d$  is 1.

So let's determine the solutions  $(x, y, z)$  to this equation such that the gcd of  $x, y$  and  $z$  is 1. I claim that this means that the gcd of any two of the numbers  $x, y, z$  must be 1. Indeed, if  $d$  is a common factor of  $y$  and  $z$ , then  $d^2$  divides  $5z^2 - y^2 = x^2$ , so that  $d$  divides  $x$  (by unique factorization of integers). Similarly, any common divisor of  $z$  and  $x$  must divide  $y$ . Finally, if  $p$  is a prime that divides both  $x$  and  $y$  then  $p^2$  divides  $x^2 + y^2 = 5z^2$ . If  $p \neq 5$ , then  $p^2$  divides  $z^2$  and hence  $p$  divides  $z$ . If  $p = 5$ , then  $p^2 | 5z^2$  implies that  $p$  divides  $z^2$  and so once again,  $p$  divides  $z$ . So we may conclude that in fact the gcd of any two numbers  $x, y, z$  must be 1.

Next, note that we can write  $(x + yi)(x - yi) = (1 + 2i)(1 - 2i)z^2$ . Since  $\mathbb{Z}[i]$  is Euclidean, it has the unique factorization property.

I claim that there's no prime in  $\mathbb{Z}[i]$  that divides both  $(x + yi)$  and  $(x - yi)$ , that is, these two elements are relatively prime. If there existed a prime  $\alpha$  that divided both of these then  $\alpha$  would also divide their sum and their difference, so  $\alpha$  would divide  $2x$  and  $2yi$ . But since  $\gcd(x, y) = 1$ , we see that  $\alpha$  must divide 2, so  $\alpha = (1 + i)$ . Note that  $1 + i$  divides  $x + yi$  if and only if  $x$  and  $y$  have the same parity, i.e., they are both even or they are both odd. Since  $\gcd(x, y) = 1$ , we see that they must both be odd, but then  $x^2 \equiv y^2 \equiv 1 \pmod{4}$  and so  $x^2 + y^2 \equiv z^2 \equiv 2 \pmod{4}$  which is impossible since a square of an integer can be congruent to either 0 or 1 mod 4 (so it can't be congruent to 2 mod 4).

So now we see that  $(x + yi)$  and  $(x - yi)$  are coprime, we see that (by unique factorization in  $\mathbb{Z}[i]$ ) we must have

$$\begin{aligned} x + yi &= \pm(1 + 2i)(r + si)^2 \text{ or} \\ x + yi &= \pm i(1 + 2i)(r + si)^2 \text{ or} \\ x + yi &= \pm(1 - 2i)(r + si)^2 \text{ or} \end{aligned}$$

$$x + yi = \pm i(1 - 2i)(r + si)^2$$

By looking at the real and imaginary parts (in each case) we get the formulas for  $x$  and  $y$ :

$$x = \pm(r^2 - s^2 - 4rs) \text{ and } y = \pm(2rs + 2r^2 - 2s^2) \text{ or}$$

$$z = \pm(2rs + 2r^2 - 2s^2) \text{ and } y = \pm(r^2 - s^2 - 4rs) \text{ or}$$

$$x = \pm(r^2 - s^2 + 4rs) \text{ and } y = \pm(2rs - 2r^2 + 2s^2) \text{ or}$$

$$x = \pm(2rs - 2r^2 + 2s^2) \text{ and } y = \pm(r^2 - s^2 + 4rs)$$

In each case  $z = \pm(r^2 + s^2)$ .

Also note that  $2rs \pm (2r^2 - 2s^2)$  is even for any choice of  $r$  and  $s$ , and so  $r^2 - s^2 \pm 4rs$  must be odd, and so  $r^2 - s^2$  must be odd. This means that  $r$  and  $s$  must have opposite parity. So if we require  $x$  to be odd and  $y$  to be even (so that we don't count  $(x, y, z)$  and  $(y, x, z)$  as distinct solutions) and if we do not take into account the  $\pm$  signs in the formulas above (we understand that if  $(x, y, z)$  is a solution to this equation, then so is  $(\pm x, \pm y, \pm z)$  for any choice of signs) then we can write down the answer as follows:

$$x = (r^2 - s^2 - 4rs) \text{ and } y = (2rs + 2r^2 - 2s^2) \text{ and } z = (r^2 + s^2) \text{ and}$$

$$x = (r^2 - s^2 + 4rs) \text{ and } y = (2rs - 2r^2 + 2s^2) \text{ and } z = (r^2 + s^2).$$

In both cases  $r$  and  $s$  have the opposite parity (one of them must be even while the other one is odd)

So this is a list of all primitive solutions to this equation. If  $(x, y, z)$  is any solution to this equation (not necessarily primitive), then let  $d$  be the gcd of  $x$ ,  $y$  and  $z$ , and note that  $(x, y, z) = d \cdot (x/d, y/d, z/d)$  and that  $(x/d, y/d, z/d)$  is a primitive solution to the given equation (and hence, it is given by one of the formulas listed above). So this gives us all the solutions to the given equation.

Problem 5.

We follow the hint and begin by finding a lower bound for  $|f(a/q)| = |(a/q)^2 - (a/q) - 1| = |a^2 - aq - q^2|/q^2$ . Note that  $a^2 - aq - q^2 \neq 0$ . If it were equal to 0, then  $a^2 = aq + q^2$ , and since  $aq + q^2$  is clearly divisible by  $q$ , it would follow that  $a^2$  is divisible by  $q$ , contradicting the fact that  $a^2$  and  $q$  are coprime (since  $a$  and  $q$  are coprime).

Thus,  $|a^2 - aq - q^2| \geq 1$  and so  $|f(a/q)| \geq (1/q^2)$ . So we found a lower bound for  $|f(a/q)|$

Next, consider  $|f(\phi) - f(a/q)|$ . On one hand, since  $f(\phi) = 0$ , this expression is just equal to  $|f(a/q)|$  and thus  $|f(\phi) - f(a/q)| \geq (1/q^2)$ . On the other hand,  $|f(\phi) - f(a/q)| = |\phi^2 - \phi - 1 - (a/q)^2 + (a/q) + 1| = |\phi - (a/q)| \cdot |\phi + (a/q) - 1|$ . So we conclude that  $|\phi - (a/q)| \cdot |\phi + (a/q) - 1| \geq (1/q^2)$ . By assumption, we have  $|\phi - (a/q)| \leq (c/q^2)$  and therefore, we get

$$(c/q^2) \geq |\phi - (a/q)| \geq 1/(q^2|\phi + (a/q) - 1|). \text{ This means that}$$

$c \geq 1/(|\phi + (a/q) - 1|)$ . Note that  $\phi - 1 > 0$  and  $(a/q) > 0$  (Indeed,  $(a/q) \geq \phi - (c/q^2) \geq \phi - (1/q^2\sqrt{5}) = [q^2\sqrt{5} + 5q^2 - 1]/[2q^2\sqrt{5}] > 0$ ), and therefore we get  $c \geq 1/(\phi + (a/q) - 1)$ . Since we have  $(a/q) \geq \phi + (c/q^2)$ , we see that

$$(a/q) + \phi - 1 \geq 2\phi - 1 + (c/q^2) \text{ and therefore}$$

$c \geq 1/[2\phi - 1 + (c/q^2)] = 1/[\sqrt{5} + (c/q^2)]$ . This tells us that  $c\sqrt{5} + (c/q^2) \geq 1$ . From this we see that there are only finitely many integers  $q$  satisfying this condition. (The point is that as  $|q|$  gets bigger and bigger,  $(c/q^2)$  gets smaller and smaller, so eventually  $(c/q^2)$  will be less than  $1 - c\sqrt{5}$ ). Formally, note that  $(c/q^2) \geq 1 - c\sqrt{5}$  and hence  $|1/q| \geq (1 - c\sqrt{5})/c$  and so  $|q| \leq c/(1 - c\sqrt{5})$ , in other words,  $-c/(1 - c\sqrt{5}) \leq q \leq c/(1 - c\sqrt{5})$ . But there are only finitely many integers in the interval  $[-c/(1 - c\sqrt{5}) ; c/(1 - c\sqrt{5})]$  so there are only finitely many choices for  $q$ . And then for each  $q$  in this interval, the inequality  $|\phi - (a/q)| \leq (c/q^2)$  tells us that  $q(\phi - (c/q^2)) \leq a \leq q(\phi + (c/q^2))$  and so there are only finitely many choices for  $a$ . So we have only finitely many choices for  $q$ , and for each  $q$  we have finitely many choices for  $a$ . Thus, there are only finitely many rationals  $a/q$  with  $(a, q) = 1$  such that  $|\phi - (a/q)| \leq (c/q^2)$  holds, as was to be shown.