Basic Algebra 1
Solutions to Assignment 2

October 14, 2013

(1) $R = \{a + b\sqrt{-5} | a, b \in \mathbb{Z}\}$ is a subset of the complex numbers. Any two elements of R, then, can be added and multiplied as elements of $\mathbb{C}$, with the result of each operation, an element of $\mathbb{C}$. But does the sum and the multiple belong to R? Let us check: Take $a + b\sqrt{-5}$ and $c + d\sqrt{-5}$ in R $(a, b, c, d \in \mathbb{Z})$

$$(a + b\sqrt{-5}) + (c + d\sqrt{-5}) = (a + c) + (b + d)\sqrt{-5} \in R,$$

and

$$(a + b\sqrt{-5})(c + d\sqrt{-5}) = ac - 5bd + (ad + bc)\sqrt{-5} \in R.$$

since $a + c, b + d, ac - 5bd, ad + bc \in \mathbb{Z}$.

So R is endowed with the addition and multiplication operations, which inherit many of their properties, namely commutativity, associativity of addition and multiplication and distributivity, from the corresponding properties of addition and multiplication on the complex numbers; for example for $x, y \in R$, since $x, y \in \mathbb{C}$ we have $x + y = y + x$ in $\mathbb{C}$ which implies that the equality also holds in R.

Now the neutral elements of addition and multiplication in $\mathbb{C}$ (0 and 1 resp.) are elements of R, $(0 = 0 + 0\sqrt{-5}$ and $1 = 1 + 0\sqrt{-5},)$ and for any $a + b\sqrt{-5}$, its additive inverse in $\mathbb{C}$, $(-a) + (-b)\sqrt{-5}$ is also in R. This proves that addition and multiplication of R has neutral elements and any element in R has an additive inverse in R. So R is a ring.

Now we prove that $p = 3$ is a prime (with the given definition); assume e is a divisor of 3, so that $3 = ef$ for some $f \in R$. We should show that $e = \pm 1$ or $\pm p$.

First we introduce the following auxiliary map from R to $\mathbb{Z}$.

$$n : R \to \mathbb{Z}$$

$$n(a + b\sqrt{-5}) = a^2 + 5b^2.$$

One can check by direct computation that for any $a, b, c, d \in \mathbb{Z}$,

$$n((a + b\sqrt{-5})(c + d\sqrt{-5})) = n(a + b\sqrt{-5})n(c + d\sqrt{-5}).$$

Let $e = a + b\sqrt{-5}$ and $f = c + d\sqrt{-5}$ for a, b, c, d in $\mathbb{Z}$. Then

$$9 = n(3) = n(ef) = n(e)n(f) = (a^2 + 5b^2)(c^2 + 5d^2).$$

Thus, by unique factorization in $\mathbb{Z}$, we deduce $n(e) = a^2 + 5b^2$ should be 1, 3 or 9. Let us consider each case separately;

If $a^2 + 5b^2 = 3$, then b is necessarily zero since otherwise $a^2 + 5b^2$ would be bigger than 3, as a^2 and $b^2 \geq 0$. But then we should have $a^2 = 3$ but there is no $a \in \mathbb{Z}$ that solves this equation and so there is no $e \in R$ with $n(e) = 3$. So $n(e)$ is either 1 or 9.

If $a^2 + 5b^2 = 1$, we should have $b = 0$ by the same argument as above, and hence $a = \pm 1$. So $e = \pm 1$.

If $a^2 + 5b^2 = 9$, then $c^2 + 5d^2 = 1$ and hence by the above case $f = \pm 1$ and as $3 = ef$ we have $e = \pm 3$. This concludes the proof that 3 is prime.

Now observe that 3 divides $(1 + \sqrt{-5})(1 - \sqrt{-5}) = 6$ but 3 does not divide neither $1 + \sqrt{-5}$ nor $1 - \sqrt{-5}$ since $n(3) = 9$ does not divide $n(1 + \sqrt{-5}) = n(1 - \sqrt{-5}) = 6$.

(2) a. We want to solve the equation $4x \equiv 3 \bmod 7$. We first observe that 4 and 7 are relatively prime (so we know the equation has a unique solution mod 7,) and so 4 is invertible in $\mathbb{Z}/7\mathbb{Z}$. In fact, one can easily observe (or use Euclidean algorithm, if one wishes!) that $1 = 2 * 4 + (-1) * 7$ and so 2 is the inverse to 4 mod 7. Now we multiply both sides of the equation to get

$$(2)(4x) \equiv (2)(3) = 6 \quad mod(7).$$

But the left hand side is congruent to x and so we have

$$x \equiv 6 \quad mod(7).$$

b. To solve $5x \equiv 2 \bmod 11$, we again have $gcd(5, 11) = 1$ and that $(-2) * 5 + 1 * 11 = 1$ and hence $5^{-1} = -2$ in $\mathbb{Z}/11\mathbb{Z}$. So we multiply both sides of the equation by -2 to get

$$x \equiv (-2)(5x) \equiv (-2)(2) = -4 \equiv 7 \quad mod(11).$$

c. $3x \equiv 6 \bmod 15$

Here $gcd(3, 15) = 3$, which divides 6. So we know that the equation has 3 solutions mod 15. To solve the equation we look at the auxiliary equation $x \equiv 2$ mod 5, which is gotten by dividing the original equation (including the modulus) by 3=gcd(3,15). But this equation has the obvious solution $x \equiv 2 \bmod 5$, which mod 15 has the following three solutions; 2 , 2+5=7 and 2+2*5=12.

d. $6x \equiv 14 \bmod 21$ This time we have $gcd(6, 21) = 3$ but 3 does not divide 14. So this equation has no solution mod 21.

(3) We wish to show that $a^5 \equiv a \bmod 30$. But this is equivalent to showing that 30 divides $a^5 - a$.

We have 30=2*3*5. Since (2,3)=(2,5)=(3,5)=1, to show 30 divides $a^5 - a$ it suffices to show $a^5 - a$ is divisible by any of the three primes, 2, 3 and 5.

We have

$$\begin{aligned} a^5 - a &= a(a^4 - 1) && (1)\\ &= a(a^2 + 1)(a^2 - 1) && (2)\\ &= a(a^2 + 1)(a - 1)(a + 1) && (3) \end{aligned}$$

From (3) we can see that $a^5 - a$ is divisible by 2, since one of the two consecutive integers a and $a + 1$ are even and hence divisible by 2. Also one of the three consecutive integers $a - 1, a$ and $a + 1$ is divisible by 3 and so $a^5 - a$ which is divisible by the multiple of the three numbers is also divisible by 3.

To prove $a^5 - a$ is divisible by 5 we use (2) and will show that either $a, a^2 - 1$ or $a^2 + 1$ is divisible by 5; If a is not divisible by 5, then $a \equiv \pm 1$ or ± 2 mod 5 (since $\{0, \pm 1, \pm 2\}$ is a complete set of residues mod 5). So $a^2 \equiv (\pm 1)^2 = 1$ or $(\pm 2)^2 = 4 \equiv -1 \bmod 5$. In the first case $a^2 - 1$ is divisivle by 5 and in the second case $a^2 + 1$ is divisible by 5.

(4) First, by FLT we know that for any integer not divisible by 13 we have $a^{12} \equiv 1 \bmod 13$.

claim For any such a the smallest positive integer, d, such that $a^d \equiv 1 \bmod 13$, is a divisor of 12.

Proof Assume d=12q+r for $0 \leq r < d$. If $r \neq 0$, we'd have

$$1 = a^{12} = a^{dq+r} = (a^d)^q a^r = 1^q a^r = a^r.$$

But this is a contradiction, since we have assumed that d is the smallest positive integer such that $a^d \equiv 1$. So $r = 0$ and 12 is divisible by d.□

Now for any given a if the corresponding d equals 12 then the set $\{1, a, a^2, ..., a^{11}\}$ cotains exactly twelve distinct non-zero residues mod 13, since if $a^i \equiv a^j \bmod 13$, for $0 \leq i < j \leq 11$, as a is invertible (not divisible by 13) we would have $a^{j-i} \equiv 1$ which contradicts the fact that $a^{d=12}$ is the smallest power of a that equals 1. This says that the set $\{1, a, a^2, ..., a^{11}\}$ contains exactly the non-zero elements of $\mathbb{Z}/13\mathbb{Z}$, and so every non-zero element can be written as a power of such a.

So for example 2 is one such number since $2^2 = 4, 2^3 = 8, 2^4 = 16 \equiv 3$ and $2^6 = 2^4 2^2 \equiv 12 \equiv -1$ and so (using the claim above) 2^{12} is the smallest positive power of 2 that equals 1. (Of course you could have written down all powers of 2 up to 11 and observed that none of them equals 1. But for primes bigger than 13, using the claim might be a better idea!)

But there exist no such number in $\mathbb{Z}/24\mathbb{Z}$, since if a is a non-zero residue mod 24, if it is prime to 24, then all powers of a will be prime to 24 and so for example the class of 2 cannot be equal to any power of a. And if a was not prime to 24, then any power of a will also be not prime to 24 so for example 5 cannot be expressed as a power of such a.

(5) $a^2 = b^2$ in $\mathbb{Z}/n\mathbb{Z}$ is equivalent to $n|a^2 - b^2$. But if n is a prime and $n|a^2 - b^2 = (a-b)(a+b)$ then by Gauss' Lemma $n|a-b$ or $n|a+b$ which means that in $\mathbb{Z}/n\mathbb{Z}$ either $a = b$ or $a = -b$.

But take $n = 21 = 3 * 7$, and $a = 10$ and $b = 4$. Then $a^2 = 100 \equiv 16 = b^2$ mod 21, but $10 \not\equiv 4$ and $10 \not\equiv -4$ mod 21.

(6) Invertible elements in $\mathbb{Z}/24\mathbb{Z} = \{0, 1, ..., 23\}$ are all the elements in the set that are prime to 24,i.e.

$$\{1, 5, 7, 11, 13, 17, 19, 23\}.$$

And similarly invertible elements in $\mathbb{Z}/9\mathbb{Z}$ are

$$\{1, 2, 4, 5, 7, 8\}.$$

(7) The idea is to compute 2^{437} in $\mathbb{Z}/437\mathbb{Z}$ and observe that it is not equal to 2 in this ring. Whereas if 437 was a prime, by FLT 2^{437} would be congruent to 2 mod 437.

To do the computation we first write 437 in base 2;

$$437 = 256 + 128 + 32 + 16 + 4 + 1 = 2^8 + 2^7 + 2^5 + 2^4 + 2^2 + 1.$$

Then we have

$$2^{437} = 2^{2^8+2^7+2^5+2^4+2^2+1} = 2^{2^8}2^{2^7}2^{2^5}2^{2^4}2^{2^2}2^1.$$

So it suffices to compute 2^{2^i} mod 437 for $0 \leq i \leq 8$. So we list these values

below (using a calculator and observing that $2^{2^i} = 2^{2^{(i-1)}2} = (2^{2^{(i-1)}})^2$)

$$\begin{aligned}
i = 0 : &\quad 2^{2^i} = 2 \\
i = 1 : &\quad 2^{2^i} = 4 \\
i = 2 : &\quad 2^{2^i} = 16 \\
i = 3 : &\quad 2^{2^i} = 256 \\
i = 4 : &\quad 2^{2^i} = (256)^2 \equiv -14 \\
i = 5 : &\quad 2^{2^i} \equiv (-14)^2 \equiv 196 \\
i = 6 : &\quad 2^{2^i} \equiv (196)^2 \equiv -40 \\
i = 7 : &\quad 2^{2^i} \equiv (-40)^2 \equiv 289 \\
i = 8 : &\quad 2^{2^i} \equiv (289)^2 \equiv 54
\end{aligned}$$

So we have

$$\begin{aligned}
2^{437} &= 2^{2^8} 2^{2^7} 2^{2^5} 2^{2^4} 2^{2^2} 2^1 \\
&= 54 * 289 * 196 * (-14) * 16 * 2 \\
&\equiv 279 \\
&\not\equiv 2
\end{aligned}$$

So 437 is not a prime.

(8) First note that $1729 = 7 * 13 * 19$. To prove that for all a, $a^{1729} \equiv a \bmod 1729$, we should show that 1729 divides $a^{1729} - a$, and for that it suffices to show that any of the primes 7, 13 and 19 divides $a^{1729} - a$, or $a^{1729} \equiv a \bmod p$ for p=7, 13 and 19.

case p=7 If $(a, 7) = 1$, we know $a^6 \equiv 1$, mod 7, by FLT, and that $1729 = 288 * 6 + 1$, so

$$a^{1729} = (a^6)^{288} a \equiv (1)^{288} a = a. \quad mod \quad 7.$$

And if $7|a$ then $a^{1729} \equiv 0 \equiv a \bmod 7$.

case p=13 Again if $(a, 13) = 1, a^{12} \equiv 1 \bmod 13$ and $1729 = 12 * 144 + 1$, so

$$a^{1729} = (a^{12})^{144} a \equiv (1)^{144} a = a. \quad mod \quad 13.$$

And if $13|a$, then $a^{1729} \equiv 0 \equiv a$.

case p=19 If $(a,19)=1, a^{18}\equiv 1 \bmod 19$ and $1729=18*96+1$, so

$$a^{1729}=(a^18)^{96}a\equiv(1)^{96}a=a. \quad mod \quad 19.$$

And if $19|a$, then $a^{1729}\equiv 0\equiv a$.

(9) Assuming p is an odd prime, we have $(p-1)/2\in\mathbb{Z}$ and so $b=a^{(p-1)/2}\in\mathbb{Z}$. Now $b^2=a^{p-1}\equiv 1 \bmod$ p, and so b is a root of the polynomial $f(x)=x^2-1$ in $\mathbb{Z}/p\mathbb{Z}$.

But f is a polynomial of degree 2 and so has at most two roots in the field $\mathbb{Z}/p\mathbb{Z}$. Since 1 and -1 are roots of f in this field, this implies that b should be equal to one or the other. so $b=\pm 1$.

For the second part of the question, again we observe that if $p-1=2^rm$, then $(p-1)/2^i$ is an integer for all $0\le i\le r$, and the sequence in question is a sequence of integers. Now if we set $b_i=a^{(p-1)/2^i}$, then we have $b_0\equiv 1$, by FLT, so the sequence starts with a one. Further, $b_i=b_{i+1}^2$, so if $b_i\equiv 1$ then b_{i+1} is a root of f mod p and so is congruent to ± 1, by the discussion above. This proves that the sequence starts with a sequence of 1's (mod p) and then the first one that is not congruent to 1, should be -1.

To check that this does not hold for $p=1729$ we write $p-1=1728=2^627$. Then we look at the sequence

$$(2^{1728}, 2^{1728/2}, ..., 2^{1728/2^4}, 2^{1728/2^5}, 2^{1728/2^6=27}),$$

and will see that mod p it equals $(1,...,1,-664,645)$. So unlike the case where p was a prime, here the first entry after the string of 1's, is not -1.

To compute 2^{27} we use the same method as in question(7). We have the following table

$$\begin{aligned} i=0: &\qquad 2^{2^i}=2\\ i=1: &\qquad 2^{2^i}=4\\ i=2: &\qquad 2^{2^i}=16\\ i=3: &\qquad 2^{2^i}=256\\ i=4: &\qquad 2^{2^i}=(256)^2\equiv -166. \end{aligned}$$

So $b_6=2^{27}=2^{16+8+2+1}=2^{2^4}2^{2^3}2^22$ equals $(-166)*256*4*2\equiv 645$.
Then $b_5\equiv b_6^2\equiv(645)^2\equiv -664$.
And $b_4\equiv b_5^2\equiv(-664)^2\equiv 1$.
Obviously because of the recursive formula, all the entries to the left of b_4 are 1.

(10) So let's look at the set of all people whom the mathematician loves; let's call this set A. But then by the mathematician's description, this set coincides with the set of all people who don't love him! Let's call this latter set B. So we have

$$A = \{\text{people whom the mathematician loves}\}$$
$$B = \{\text{people who don't love the mathematician}\}$$

and we know $A = B$.

Now let's see whether the mathematician himself belong to the set A or not! Does he love himself or not?!

If he loves himself, then he belongs to the set A. But then he cannot belong to the set B since this set contains only people who don't love him! But $A = B$ and that's a contradiction!

Similarly, if he doesn't love himself, then he doesn't belong to the set A. But he belongs to the set B and again this contradicts the fact that $A = B$.