MATH 3030, Abstract Algebra
FALL 2012
Toby Kenney

Homework Sheet 8

Due: Wednesday 21st November: 3:30 PM

Basic Questions

1. *Find the remainder of* 6^{12345} *when divided by 13.*

   We know that $6^{12} \equiv 1 \pmod{13}$, so $6^{12345} \equiv 6^{11} \pmod{13}$. We calculate $6^2 \equiv 10 \pmod{13}$, $6^4 \equiv 9 \pmod{13}$, and $6^8 \equiv 11 \pmod{13}$, so that $6^{11} \equiv 6^8 \times 6^2 \times 6 \equiv 11 \times 10 \times 6 \equiv 10 \pmod{13}$.

2. *Find the remainder when* 9^{123456} *is divided by 91. [Hint:* $91 = 7 \times 13$*; see Q. 7.]*

   By Euler's formula, we know that $9^{\phi(91)} \equiv 1 \pmod{91}$. By question 7(b), we have that $\phi(91) = (7-1)(13-1) = 72$. Now $123456 \equiv 45 \pmod{72}$. Furthermore $9 = 3^2$, so $9^{123456} \equiv 3^{18} \pmod{91}$. We compute $3^4 \equiv 81 \equiv -10 \pmod{91}$, so $3^8 \equiv 100 \equiv 9 \pmod{91}$ and $3^{16} \equiv 81 \pmod{91}$, so $3^{18} \equiv -10 \times 9 \equiv -90 \equiv 1 \pmod{91}$.

   Alternatively: we check $9^2 \equiv -10 \pmod{91}$ and $9^3 \equiv -90 \equiv 1 \pmod{91}$, and since $123456 \equiv 0 \mod 3$, we get $9^{123456} \equiv 1 \pmod{91}$.

3. *Find the last digit of* $3^{3^{3^{3^{3^{3^{3^{3^{3^{3^{3^{3}}}}}}}}}}}$ *(in base 10).*

   The last digit is the remainder when $3^{3^{3^{3^{3^{3^{3^{3^{3^{3^{3^{3}}}}}}}}}}}$ is divided by 10, but we have $3^{\phi(10)} \equiv 1 \pmod{10}$, so we need to compute $3^{3^{3^{3^{3^{3^{3^{3^{3^{3^{3}}}}}}}}}}$ modulo $\phi(10) = 4$. However, we know that $3^2 \equiv 1 \pmod{4}$, so the remainder of 3^n modulo 4 depends only on whether n is even or odd. Since n is a power of 3, it must be odd, so we have $3^{3^{3^{3^{3^{3^{3^{3^{3^{3^{3}}}}}}}}}} \equiv 3 \pmod{4}$, and therefore, $3^{3^{3^{3^{3^{3^{3^{3^{3^{3^{3^{3}}}}}}}}}}} \equiv 3^3 \equiv 7 \pmod{10}$, so the last digit is 7.

4. *Solve:*

   (a) $15x \equiv 11(mod 33)$

   15 and 33 are both divisible by 3, but 11 is not, so there are no solutions.

   (b) $5x \equiv 11(mod 33)$

5 is coprime to 33, so it is invertible in $\mathbb{Z}_{33}$. Now we have that $5 \times 11 \equiv -11 \pmod{33}$, so that $x \equiv -11 \equiv 22 \pmod{33}$ is the solution.

5. *Describe the field of quotients of the integral domain* $\{a + b\sqrt{2}i | a, b \in \mathbb{Z}\}$.

   The field of quotients consists of all real numbers of the form $\frac{a+b\sqrt{2}i}{c+d\sqrt{2}i}$. We can multiply the denominator by $c - d\sqrt{2}i$ to get numbers of the form $\frac{(a+b\sqrt{2}i)(c-d\sqrt{2}i)}{c^2+2d^2}$. This gives the set of numbers of the form $x + y\sqrt{2}i$ for x and y rational numbers.

6. *Describe the field of quotients of the integral domain* $\{a + b\sqrt{5} | a, b \in \mathbb{Z}\}$.

Standard Questions

7. *Let $n = pq$ where p and q are prime.*

   (a) Show that $\phi(n) = (p-1)(q-1)$.

   In the collection of numbers from $\{1, \ldots, pq\}$, p are divisible by q, and q are divisible by p, while 1 is divisible by both p and q. Therefore, $p+q-1$ numbers are not coprime to pq. The remaining $pq-p-q+1 = (p-1)(q-1)$ are coprime to pq, so $\phi(pq) = (p-1)(q-1)$.

   Alternatively, for any x coprime to pq, we can look at the remainders when x is divided by p and by q. By the Chinese remainder theorem, there is exactly one value of x modulo pq for each pair of remainders modulo p and modulo q.

   (b) If e and $n = pq$ are known numbers, and we are told m^e modulo n, how can we recover the value of m?

   We know that $m^{\phi(n)} \equiv 1 \pmod{n}$, so that if $x \equiv 1 \pmod{\phi(n)}$, then we have $m^x \equiv m \pmod{n}$. Therefore, we need to find the inverse e' of e in $\mathbb{Z}_{(p-1)(q-1)}$, so that $ee' \equiv 1 \pmod{(p-1)(q-1)}$. Now we have that $(m^e)^{e'} = m^{ee'} \equiv m \pmod{n}$, so we can recover m by raising m^e to the power e' modulo n.

   [This is the RSA encryption algorithm. It is extensively used for secure communication over the internet. The important point here is that recovering m (which is the encrypted message) depends upon the knowledge of the prime factors p and q, which are difficult to determine from the product n, for large p and q.

8. *Prove Wilson's Theorem, that if p is prime, then $(p-1)! \equiv -1 \pmod{p}$. [Hint: first show that 1 and -1 are the only self-inverse elements of $\mathbb{Z}_p$.]*

   The elements 1 and -1 are self-inverse in $\mathbb{Z}_p$, and all other elements can be partitioned into inverse pairs $\{a, a^{-1}\}$. Therefore, when we take the product of all non-zero elements of $\mathbb{Z}_p$, it is of the form $1 \times -1 \times a_1 \times {a_1}^{-1} \times \cdots \times a_n \times {a_n}^{-1} = 1 \times -1 \times 1 \times \cdots \times 1 = -1$.

9. *Prove the distributive law holds in the field of quotients of an integral domain.*

   Let D be an integral domain, and let F be its field of quotients. We want to show that for any elements $[(a, a')]$, $[(b, b')]$ and $[(c, c')]$ in F, we have that $[(a, a')]\,([(b, b')] + [(c, c')]) = [(a, a')][(b, b')] + [(a, a')][(c, c')]$. Now we know that $[(a, a')]\,([(b, b')] + [(c, c')]) = [(a, a')][(bc' + cb', b'c')] = [(a(bc' + b'c), a'b'c')]$, while $[(a, a')][(b, b')] + [(a, a')][(c, c')] = [(ab, a'b')] + [(ac, a'c')] = [(aba'c' + aca'b', a'ba'c)]$. However, multiplying both elements of the first pair by a', we easily see that these are equivalent elements of F.

10. *If D' is a subdomain of D, must the field of quotients of D' be a subfield of the field of quotients of D?*

    The field of quotients of D consists of equivalence classes of pairs (a, b) of elements of D. The field of quotients of D' consists of equivalence classes of pairs (a', b') of elements of D'. It is clear that pairs of elements of D' are also pairs of elements of D. However, we need to show that if two pairs of elements of D' are equivalent as pairs of elements in D, then they are also equivalent as pairs of elements in D'. However, this is clear, since the equation $a_1b_2 = a_2b_1$ holds in D' if and only if it holds in D.

Bonus Questions