Compiled Exercises

Jose Capco (jcapco@risc.jku.at)

1. Let R be a commutative unitary ring and $f \in R[x] \backslash R$ then

a.) For an $a \in R$ there is a unique $g \in R[x]$ such that $f = (x-a)g + f(a)$. Show that this is not necessarily true of if we replace R by a non-commutative ring.

b.) If R is a domain and $a_1, a_2, \ldots, a_k \in R$ are distinct zeros of f, then

$$\prod_{i=1}^{k}(x - a_i) \mid f$$

Show that this is not necessarily true if we remove the requirement that R is a domain.

2. Write a computer program that takes $a \in \mathbb{N}$ and $n \in 2\mathbb{N}+1$ and outputs the Jacobi symbol $\left(\frac{a}{n}\right)_J$.

Hint: Use quadratic reciprocity laws and factorize $a = 2^s t$ where t is odd.

3.

a.) Prove that for an odd prime p and for $k \in \mathbb{N}$ the multiplicative group $(\mathbb{Z}/2p^k)^*$ is cyclic.

b.) Write a program that finds the primitive root mod n if $(\mathbb{Z}/n)^*$ is cyclic.

c.) Write a method `ArtinCounts`(a, x) that takes a non-square $a \geq 2$ and $x \in \mathbb{N}$ and counts all prime numbers $p \leq x$ for which a is a primitive root mod p. For a non-square $a \in \mathbb{N}$, plot `ArtinCounts`(a, x) with increasing x (try this for different non-square a).

4.

a.) Show that a Carmichael number must have at least three prime factors.

b.) Show that if there are three primes of the form $6m+1$,$12m+1$ and $18m+1$ for some $m \in \mathbb{N}$ then their product is a Carmichael number. In your opinion (with justification), how many such Carmichael numbers would exist?

c.) Let $C(x)$ be the number of Carmichael numbers less or equal $x \in \mathbb{R}^+$. Plot $C(x)$ over the positive real line and verify (however you can) that for sufficiently large x, we have $C(x) > x^{2/7}$ (if this is proven, then one proves the infinitude of Carmichael numbers).

5. Let X be an indeterminate, p be an odd prime and $m \in \mathbb{N}$ such that $p \nmid m$ and suppose $e \in \mathbb{N}$, then prove that the number of solutions for $X^m = 1 \bmod p^e$ in the ring $\mathbb{Z}/p^e$ is given by

$$\gcd(m, \phi(p^e)) = \gcd(m, p^{e-1}(p-1))$$

Find a general statement giving the number of roots of unity modulo a composite number.

6. Write a program that finds the least set of bases needed to check if a number $n \leq 100$ is a prime number using the Miller-Rabin test.

7. Use Wilson's to show

a.) p and $p+2$ are two primes (i.e. twin-primes) iff $4(p-1)! = -4 - p \bmod p(p+2)$

b.) A number $p \in 2\mathbb{N}+1$ is a prime iff $\left(\left(\frac{p-1}{2}\right)!\right)^2 = (-1)^{(p+1)/2} \bmod p$

8. Prove that for any $n \in 2\mathbb{N}+1$ we can find an $r \in \mathbb{N}$ such that $(r,n)=1$ and the order of n in $(\mathbb{Z}/r)^*$ is greater than $\log_2^2 n$. In fact, r can be search in the interval $[1, \log_2^5 n]$

9. Write an algorithm that modifies Eratosthenes sieving algorithm to get B-smooth numbers up to n for given B and n.

10. In the Miller-Rabin test, the set of (composite witnesses) for an odd composite n is

$$\{a \in \mathbb{N} : 1 \leq a < n \text{ and } a \text{ does not satisfy } (*)\}$$

where $(*)$ is the criterion for a in the Miller-Rabin test (see Lecture 02). The minimum number in this set is called the *least witness* for n and denoted $w(n)$. For most numbers $w(n) = 2$. Use the inequality of Pomerance and Konyagin to prove a result of Granville:

If a composite odd number n is not square-free (so there is a prime $p \in \mathbb{P}$ such that $p^2 \mid n$) then $w(n) < \ln^2 n$.

11. Suppose $n = pq$ is an odd composite number and that $|p-q| < n^{1/4}$ as in the above procedure. Find the maximum number of steps in Fermat factorization method that is needed to obtain p and q.

12. Let $n \in 2\mathbb{N}+1$ be a composite number and $p, q \in P$ be such that $p \neq q$ and $pq \mid n$. Let $B \in \mathbb{R}$ such that $B > 0$ such that $p-1$ is B-power-smooth but $q-1$ is not B-power-smooth Prove that

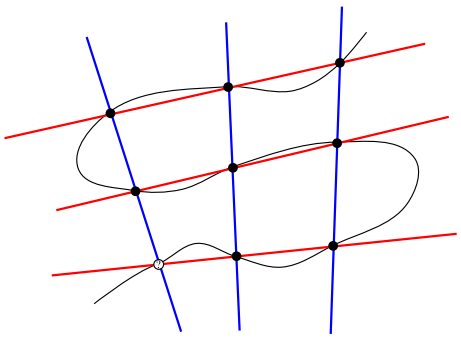
$$\#\{a \bmod n : a^{\beta(B)} = 1 \bmod n\}/\phi(n) \leq \frac{1}{2}$$

13. Given an elliptic curve E, show that O is a flex point i.e. if E is regarded as a projective plane curve and L is the tangent line at O then $I(O, E \cap L) = 3$.

14. The Cayley-Bacharach theorem states that if C_1, C_2 are two cubic curves in the projective plane such that $\#(C_1 \cap C_2) = 9$ and if C_3 is a third cubic curve then

$$\#(C_1 \cap C_2 \cap C_3) \geq 8 \Rightarrow C_1 \cap C_2 \cap C_3 = C_1 \cap C_2$$

i.e. the ninth point will also be in C_3 (see figure below).



Use this result to prove associativity of addition of points in an elliptic curve E.

15. Write the addition formula for points of elliptic curves given by an equation in the Weierstrass long form. Write an algorithm that adds points of an elliptic curve given by this general form.

16. Suppose $E : y^2 = x^3 + ax + b$ be an elliptic curve over K ($\operatorname{char} K > 3$ or $\operatorname{char} K = 0$). Let $\phi : E(\bar{K}) \to E(\bar{K})$ be an isogeny with

$$\phi(x,y) = \left(\frac{p(x)}{q(x)}, y\frac{s(x)}{t(x)}\right) \qquad \gcd(p,q) = 1, \gcd(s,t) = 1$$

a.) Use the fact that (x, y) and $\phi(x, y)$ lies on E to show that

$$\frac{(x^3 + ax + b)s(x)^2}{t(x)^2} = \frac{u(x)}{q(x)^3}$$

for some $q, u \in K[x]$ with $\gcd(q, u) = 1$. Hint: Show that a common root u and q is a root of p.

b.) Suppose that $t(\alpha) = 0$, then use the fact that $x^3 + ax + b$ has no multiple root and all roots of t^2 are multiple roots to show that $q(\alpha) = 0$. In other words, show that $q(\alpha) \neq 0$ implies that $\phi(\alpha, \beta)$ is defined for any point $(\alpha, \beta) \in E$.

c.) Show that $\frac{d}{dx}\frac{p(x)}{q(x)} \equiv 0$ iff $p'(x) \equiv 0$ and $q'(x) \equiv 0$ (so if p is nonconstant in this case $\operatorname{char} K > 0$).

17. Given an elliptic curve $E : y^2 = x^3 + ax + b$ over K with $\operatorname{char} K \nmid 6$, show that $\deg[n] = n^2$

18. In the lectures we have shown that for a non-trivial separable isogeny $\phi : E_1 \to E_2$ we have the following

$$\deg \phi = \#\ker(\phi)$$

We made the use of the surjectivity of ϕ to prove this. Modify the proof without knowing that ϕ is surjective. Also, suppose that ϕ is not necessarily separable, show that $\ker \phi$ is finite in fact show

$$\#\ker(\phi) \leq \deg \phi$$

Hint: The proof is the same as the proof in Lecture 10 (only one line of argument is different).

19. Extend ECM such that you can collect which elliptic curves $E_{a,b}$ and which point $P \in E_{a,b}$ yields a factor $p \mid n$. Write a function that gives the order of such $E_{a,b}$ over $\mathbb{F}_p$ and provide some sample computation from your new algorithm.

20. If we identify finite abelian groups up to isomorphisms, how many finite abelian groups are there that have order $n \in \mathbb{N}$? (Hint: Research partition numbers).

21. Let $E : y^2 = x^3 + ax + b$ be an elliptic curve over $\mathbb{Q}$ $(a, b \in \mathbb{Z})$. Show that for any $n \in \mathbb{N}$

$$\{P \in E\backslash\{O\} \,:\, v(x_P/y_P) \geq n\} = \{P \in E\backslash\{O\} \,:\, v(x_P) \leq -2n, v(y_P) \leq -3n\} \cup \{O\}$$

More specifically show that for any point $P \in E\backslash\{O\}$

$$v(x_P) < 0 \Leftrightarrow v(y) < 0$$

and if $v(x_P) < 0$ then there is an $n \in \mathbb{N}$ such that $v(x_P) = -2n$ and $v(y_P) = -3n$.

22. Let $n \in \mathbb{N}$ and consider the elliptic curve $E_n : y^2 = x^3 - n^2 x$ over $\mathbb{Q}$. Show that

$$\operatorname{Tor}(E) = \{O, (0, 0), (-n, 0), (n, 0)\}$$

Hint: From Nagell-Lutz we know that $\#\operatorname{Tor}(E) \mid \#E(\mathbb{F}_p)$ for a good reduction of E modulo a prime p. The above is true for any good reduction and you conclude this by counting $\#E(\mathbb{F}_p)$ for good reduction modulo primes $p \equiv 3 \bmod 4$.