TRENTO, A.A. 2019/20
CORSO DI ALGEBRA A
FOGLIO DI ESERCIZI # 10

Esercizio 10.1. Si consideri il seguente schema RSA, in cui Bob manda un messaggio ad Alice.

(1) Alice pensa i numeri primi $p = 23$ e $q = 31$, e calcola $n = pq$.
(2) Notate che $26^2 \leq n < 26^3$. Alice calcola $\varphi(n)$, e sceglie $r = 7$.
(3) Prendete un messaggio di otto lettere, il messaggio che Bob vuole inviare a Alice. Dividetelo in quattro gruppi di due lettere. Codificate ogni lettera come un numero fra 0 e 25, secondo lo schema $A \mapsto 0$, $B \mapsto 1$, $\dots Z \mapsto 25$. Codificate, con il metodo esposto a lezione, ogni coppia di lettere come un numero p_i compreso fra 0 e $26^2 - 1 < n$, per $i = 1, 2, 3, 4$. Ad esempio, se a, b sono le prime due lettere (già espresse come numeri), allora $p_1 = a + b \cdot 26$.
(4) Mostrate come fa Bob a crittare il messaggio, ottenendo $c_i \equiv p_i^r \pmod{n}$.
(5) Mostrate come fa Alice a decifrare il messaggio, calcolando cioè s, e ottenendo $p_i \equiv c_i^s \pmod{n}$.

Esercizio 10.2. Un altro esempio di RSA: qui voi fate la parte di Alice. Il mittente è sempre Bob.

(1) Alice sceglie i numeri primi $p = 19$ e $q = 37$, e calcola $n = pq$ e $\varphi(n)$. Notate che n è compreso fra 26^2 e 26^3, dunque si possono crittare coppie di lettere.
(2) Alice sceglie poi $r = 85$. Verificate che sia $(r, \varphi(n)) = 1$, e calcolate s, t tali che $rs + \varphi(n)t = 1$.
(3) Comunicate r, n a Bob, che dopo un po' vi manda il messaggio

$$550, 87, 182, 35, 87, 446.$$

Decifratelo.
(4) Ah, dopo aver decifrato, come spiegate l'ultima, strana lettera del messaggio di Bob?

Esercizio 10.3. L'esempio di RSA fatto a lezione.

(1) Bob sceglie i numeri primi $p = 11$ e $q = 67$, e calcola $N = p \cdot q$ e $\varphi(N)$ (fatelo anche voi.
(2) Bob sceglie $r = 283$, e calcola s, t tali che

$$rs + \varphi(N)t = 1.$$

(Fatelo anche voi.)
(3) Bob annuncia la chiave pubblica (N, r).
(4) Alice cifra il messaggio "GATTOX", e lo manda a Bob. (Fatelo anche voi.)
(5) Bob decifra il messaggio. (Fatelo anche voi.)

Esercizio 10.4 (Facoltativo). Sia $n = pq$, ove p, q sono primi distinti. Siano r, s, t tali che

$$rs + \varphi(n)t = 1.$$

Si mostri che $a^{rs} \equiv a \pmod{n}$ per ogni intero a.

Dunque questo esercizio mostra che anche se gli a_i di Bob non soddisfano $\gcd(a_i, n) = 1$, Alice può comunque ricostruirli usando $a_i \equiv a_i^{rs} = (a_i^r)^s \equiv b_i^s \pmod{n}$.

(SUGGERIMENTO: Per $\gcd(a, n) = 1$ questo segue da Eulero-Fermat, come visto a lezione. Si tratta di vedere che la congruenza di cui sopra vale anche se $\gcd(a, n) \neq 1$, e questa parte è facoltativa. In tal caso conviene pensare a cosa può essere, questo massimo comun divisore, e magari usare il Teorema Cinese.)

Esercizio 10.5. Siano p, q primi distinti, e sia $n = pq$. La probabilità che un numero $0 \leq a < n$ preso a caso sia relativamente primo con n (ovvero che $\gcd(a, n) = 1$) è

$$\frac{\varphi(n)}{n} = \left(1 - \frac{1}{p}\right) \cdot \left(1 - \frac{1}{q}\right) = 1 - \frac{1}{p} - \frac{1}{q} + \frac{1}{pq}.$$

Se $p, q \approx 10^{200}$, si dia una stima della grandezza di $\varphi(n)/n$, ovvero della piccolezza di

$$1 - \frac{\varphi(n)}{n} = \frac{n - \varphi(n)}{n},$$

che rappresenta la probabilità che un numero a preso a caso *non* sia relativamente primo con n (ovvero che $\gcd(a, n) > 1$).

Dunque questo esercizio mostra come sia estremamente improbabile che uno degli a_i di Bob *non* sia coprimo con n. In effetti, se fosse cosí facile trovare (andando per tentativi a caso) un numero $0 < a < n$ che *non* sia coprimo con n, basterebbe poi calcolare $\gcd(a, n)$, che essendo un divisore di $n = pq$ diverso 1 deve essere p o q, per riuscire a fattorizzare n.

Esercizio 10.6. Sia n un intero positivo (grande). Qual è la probabilità che un numero a preso a caso sia relativamente primo con n? Nel seguito diamo una stima, che però non è un gran che; mi riservo di sostituirla con una stima migliore.

La probabilità, come nell'esercizio precedente, è $\varphi(n)/n$. Ora se

$$n = p_1^{e_1} \cdots p_k^{e_k}$$

è la scomposizione di n come prodotto di potenze di primi p_i, con $p_i < p_j$ per $i < j$, e $e_i \geq 1$ per ogni i, allora

$$\begin{aligned} \frac{\varphi(n)}{n} &= \frac{(p_1 - 1)p_1^{e_1 - 1} \cdots (p_k - 1)p_k^{e_k - 1}}{p_1^{e_1} \cdots p_k^{e_k}} \\ &= \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right). \end{aligned}$$

Ora siano $q_1 = 2, q_2 = 3, q_3 = 5, \ldots$ tutti i numeri primi, nel loro ordine naturale. Avremo chiaramente $p_i \geq q_i$, e dunque per ogni i

$$1 - \frac{1}{p_i} \geq 1 - \frac{1}{q_i},$$

dato che per numeri x, y positivi si ha $x > y$ sse $1/y > 1/x$ sse $-1/x > -1/y$ sse $1 - 1/x > 1 - 1/y$.

Dunque

$$\frac{\varphi(n)}{n} \geq \prod_{i=1}^{k}\left(1-\frac{1}{q_i}\right) = \prod_{i=1}^{k}\frac{q_i-1}{q_i} \geq \prod_{i=1}^{k}\frac{q_{i-1}}{q_i}$$
$$= \frac{q_0}{q_1}\cdot\frac{q_1}{q_2}\cdot\frac{q_2}{q_3}\cdots\frac{q_{k-1}}{q_k} = \frac{q_0}{q_k} = \frac{1}{q_k},$$

dato che $q_i > q_{i-1}$, e dunque $q_i - 1 \geq q_{i-1}$. (Qui abbiamo preso convenzionalmente $q_0 = 1 \leq 2 - 1 = q_1 - 1$.)

Dunque scegliendo a caso un numero a fra 0 compreso e n escluso, ho probabilità almeno $1/q_k$ (ove q_k è il k-simo numero primo) di trovare che $\gcd(a, n) = 1$.

Esercizio 10.7. Sia $\alpha \in \mathbf{R}$. Definiamo

$$\lfloor \alpha \rfloor = \max\{\, x \in \mathbf{Z} : x \leq \alpha \,\}, \qquad \lceil \alpha \rceil = \min\{\, x \in \mathbf{Z} : x \geq \alpha \,\}.$$

$\lfloor \alpha \rfloor$ viene a volte anche denotato come $[\alpha]$ (niente a che fare con le classi resto, tante notazioni non sono univoche, ma dipendono dal cotesto), e chiamata la *parte intera* di α.

(1) Mostrate che $\lfloor \alpha \rfloor$ e $\lceil \alpha \rceil$ esistono.

(Suggerimento: Faccio solo il primo caso. Magari la faccio più complicata di quel che serve, ma $B = \{\, x \in \mathbf{Z} : x \leq \alpha \,\} \subseteq \mathbf{R}$ è limitato superiormente (da α), dunque ha un sup, sia b_0. Resta da vedere che $b_0 \in \mathbf{Z}$, e dunque b_0 è il massimo di B. Consideriamo l'intervallo aperto $I =]b_0 - 1/4, b_0 + 1/4[$. Siccome la lunghezza di I è minore di 1, in I c'è al più un numero intero (o magari nessuno, per quel che ne sappiamo finora). Ma dato che $b_0 = \sup(B)$ è un limite di elementi di B, $b_0 = \lim_{n\to\infty} x_n$, con $x_n \in B$, esiste N tale che $x_n \in I$ per $n \geq N$. Dato che ogni $x_n \in \mathbf{Z}$, e in I c'è al più un intero, vorrà dire che x_n è costante per $n \geq N$. Dunque il limite b_0 di questa successione è questa costante, e quindi $b_0 \in \mathbf{Z}$.)

(2) Mostrate che se $\alpha \in \mathbf{Z}$, allora

$$\lfloor \alpha \rfloor = \alpha = \lceil \alpha \rceil.$$

(3) Mostrate che se $\alpha \notin \mathbf{Z}$, allora

$$\lceil \alpha \rceil = \lfloor \alpha \rfloor + 1.$$

Esercizio 10.8. Spiegate come si fa l'elevamento a potenza (modulo N) col metodo della scrittura dell'esponente in base 2, in particolare spiegando quante operazioni (divisioni con resto, moltiplicazioni) sono necessarie.

Esercizio 10.9. Sia A un anello commutativo con unità. Sia $A^{\mathbf{N}}$ l'insieme delle successioni a valori in A. Sia $A[x]$ il sottoinsieme di $A^{\mathbf{N}}$ delle successioni definitivamente (quasi ovunque) nulle.

(1) Si mostri che $A[x]$ diventa un anello commutativo con unità, con le operazioni

$$(a + b)_k = a_k + b_k,$$

e

$$(a \cdot b)_k = \sum_{i+j=k} a_i b_j, \tag{1}$$

per $a, b \in A[x]$, e $k \in \mathbf{N}$. Dunque $a+b$ è quell'elemento di $A[x]$ che ha come k-sima componente la somma delle k-sime componenti di a e b, mentre $a \cdot b$ è quell'elemento di $A[x]$ che ha come k-sima componente $\sum_{i+j=k} a_i b_j$.

(Suggerimento: Vi faccio vedere l'associatività del prodotto, anche perché è una buona occasione per vedere quanto possa aiutare una buona notazione. Abbiamo, applicando due volte la definizione (1),

$$\begin{aligned}((a \cdot b) \cdot c)_t &= \sum_{u+k=t} (a \cdot b)_u c_k \\ &= \sum_{u+k=t} (\sum_{i+j=u} a_i b_j) c_k \\ &= \sum_{i+j+k=t} a_i b_j c_k,\end{aligned}$$

e si vede (ma fatelo!) che lo stesso risultato si ottiene calcolando $a \cdot (b \cdot c)$. Ora l'espressione $\sum_{i+j=k} a_i b_j$ si può anche riscrivere come una somma su una sola variabile, dato che $j = k - i$, nella forma $\sum_{i=0}^{k} a_i b_{k-j}$. Ma se provate a fare la dimostrazione con questa formula che vi ho appena mostrato, vedrete che dovete fare un cambio di variabili, cambio che la prima forma evita.)

(2) Mostrate che la funzione

$$\begin{aligned}\varphi : A &\to A[x] \\ \lambda &\mapsto (\lambda, 0, 0, \dots)\end{aligned}$$

è un morfismo iniettivo.

(3) Mostrate che se

$$x = (0, 1, 0, 0, \dots)$$

allora per $i \geq 1$ si ha

$$x^i = (0, \dots, 0, 1, 0, \dots),$$

ove quell'unico 1 è all'i-simo posto, cominciando a contare da 0, naturalmente.

(4) Mostrate che se $\lambda \in A$ e $a = (a_0, a_1, \dots) \in A[x]$, si ha

$$\varphi(\lambda) \cdot a = (\lambda a_0, \lambda a_1, \dots).$$

L'ultima scrittura si indica anche, nella forma di prodotto dello "scalare" λ per il "vettore" a, come λa.

(5) Mostrate che, con la notazione appena introdotta, se

$$a = (a_0, a_1, \dots, a_n, 0, 0, \dots) \in A[x],$$

allora

$$a = a_0 + a_1 x + \cdots + a_n x^n.$$

(6) Mostrate che vale il principio di identità dei polinomi, cioè

$$a_0 + a_1 x + \cdots + a_n x^n = b_0 + b_1 x + \cdots + b_n x^n$$

se e solo se $a_i = b_i$ per ogni i.

Esercizio 10.10. Sia A un anello commutativo con unità, $A[x]$ l'anello dei polinomi, $a, b \in A[x]$.

(1) Si dia la definizione di grado di a. Si mostri che la definizione di grado vale per tutti i polinomi, tranne il polinomio nullo.
(2) Si mostri che sono equivalenti
   (a) a è un polinomio di grado 0, e
   (b) a è una costante non nulla.
(3) Si mostri con un esempio che, scegliendo opportunamente A, a, b, può essere $\text{grado}(ab) \neq \text{grado}(a) + \text{grado}(b)$ per $0 \neq a, b \in A[x]$. (Addirittura potrebbe essere $a \neq 0 \neq b$ e $ab = 0$, sicché ab non ha neanche un grado.)
(4) Si mostri che se A è un dominio, allora se $0 \neq a, b \in A[x]$ si ha $ab \neq 0$, e

$$\text{grado}(ab) = \text{grado}(a) + \text{grado}(b).$$

(5) Si mostri che in particolare, se A è un dominio, anche $A[x]$ è un dominio.
(6) Si mostri che se $0 \neq a, b \in A[x]$, allora

$$\text{grado}(a + b) = \max(\text{grado}(a), \text{grado}(b)) \quad \text{se grado}(a) \neq \text{grado}(b).$$

(7) Si mostri con opportuni esempi che se $\text{grado}(a) = \text{grado}(b)$, allora può essere $a + b = 0$, e $\text{grado}(a + b)$ può assumere qualsiasi valore fra 0 e $\text{grado}(a) = \text{grado}(b)$.

Esercizio 10.11 (Proprietà universale dell'anello dei polinomi).

Sia B un anello commutativo con unità 1, e A un sottoanello di B contenente 1.

Si mostri che esiste un unico morfismo di anelli (detto morfismo di valutazione in α)

$$v_\alpha : A[x] \to B$$

tale che

$$\begin{cases} v_\alpha(c) = c & \text{per } c \in A, \text{ e} \\ v_\alpha(x) = \alpha. \end{cases}$$

Si mostri che

$$v_\alpha(a_0 + a_1 x + \cdots + a_n x^n) = a_0 + a_1 \alpha + \cdots + a_n \alpha^n,$$

per $n \in \mathbf{N}$ e $a_i \in A$.