Crittografia ed Aritmetica Modulare
– III incontro –

PLS - CAM

Padova, 31 ottobre 2014

1 Fattorizzazione unica e Divisione intera

Teorema 1.1 (FATTORIZZAZIONE UNICA)**.** *Ogni $m \in \mathbb{Z}$, $m \neq 0, 1, -1$, si scrive in modo essenzialmente unico (cioè a meno del segno e dell'ordine dei fattori) come prodotto di numeri primi*

$$m = (\pm 1)\, p_1^{e_1} p_2^{e_2} \cdots p_t^{e_t}$$

ove i $p_i \neq p_j$ (per $i \neq j$) sono (i fattori) primi (di m), e gli e_i sono esponenti interi ≥ 1.

Per esempio $-12 = -\,2^2 \cdot 3 = 2^2 \cdot (-3) = -\,3 \cdot 2^2 = -\,3 \cdot (-2)^2$.

Teorema 1.2 (DIVISIONE INTERA)**.** *Dati interi $a, n \in \mathbb{Z}$, con $n > 0$, esistono unici $q, r \in \mathbb{Z}$, con $0 \leq r < n$, tali che $a = nq + r$. Si dice che q è il quoziente e r è il resto della divisione (intera) di a per n.*

Esempi:

- Se $a = 27$ e $n = 12$, abbiamo $27 = 12 \cdot 2 + 3$, cioè $q = 2$ e $r = 3$;
- se $a = -5$ e $n = 12$, abbiamo $-5 = 12 \cdot (-1) + 7$, cioè $q = -1$ e $r = 7$;
- se $a = 36$ e $n = 12$, abbiamo $36 = 12 \cdot 3 + 0$, cioè $q = 3$ e $r = 0$.

Esercizio 1.3. *Oggi, martedì 3 aprile, alle ore 21, devo prendere un treno per la Transilvania che mi porterà a destinazione in 57 ore. In che giorno ed a che ora arriverò?*

Definizione 1.4. *Dati $a, b \in \mathbb{Z}$, diremo che "a divide b", o che "b è multiplo di a", e scriveremo $a|b$, se $b = a\,k$ per qualche $k \in \mathbb{Z}$. Cioè $a|b$ se e solo se il resto della divisione intera di b per a è eguale a zero.*

Esercizio 1.5. *Si verifichino le seguenti proprietà:*

- *se $a|b$ e $b|c$, allora $a|c$;*
- *se $a|b$ e $b|a$, allora ...*
- *se $a|b$ e $a|c$, allora $a|\beta b + \gamma c$, qualunque siano $\beta, \gamma \in \mathbb{Z}$;*
- *$1|a$ e $a|0$, per qualunque $a \in \mathbb{Z}$.*

2 Algoritmo di Euclide e Formula di Bézout

Dal Teorema di Fattorizzazione Unica segue subito che ogni coppia di interi $a, b \in \mathbb{Z}$ ammette un MASSIMO COMUNE DIVISORE $d = (a, b)$ che ha la seguente proprietà:

$d|a$ e $d|b$, ed inoltre se $d' \in \mathbb{Z}$ è tale che $d'|a$ e $d'|b$, allora necessariamente $d'|d$.

Il massimo comune divisore è dunque unico a meno del segno.

Tale (a, b) si calcola immediatamente, non appena siano note le fattorizzazioni di a e di b. Tuttavia fattorizzare un (grande) numero intero nel prodotto dei suoi fattori primi è estremamente oneroso da un punto di vista algoritmico.

ATTIVITÀ 2.1. *Dopo aver fattorizzato entrambi i numeri, si calcoli*

$$d = (24750, 3900).$$

Definizione 2.2. *Se accade che $(a, b) = 1$, si dice che a e b sono* COPRIMI.

Vi è un altro modo algoritmicamente ben più efficiente per il calcolo diretto di (a, b), senza dover passare attraverso le singole fattorizzazioni di a e b. È l'ALGORITMO DI EUCLIDE che, nella sua forma estesa, permette

di determinare non solo il massimo comune divisore di a e b, bensì anche coefficienti interi $\alpha, \beta \in \mathbb{Z}$ tali per cui

$$\boxed{d = (a, b) = \alpha\, a + \beta\, b}\ .$$

Questa è detta FORMULA DI BÉZOUT, e si rivelerà in seguito di cruciale importanza per il calcolo delle classi inverse modulo n.

Algoritmo 2.3 (EUCLIDE ESTESO)**.** *Siano $a > b > 0$ interi. Si consideri la tabella:*

	1	0	a	
$-q_1$	0	1	b	$a = bq_1 + r_1$
$-q_2$	1	$-q_1$	r_1	$b = r_1q_2 + r_2$
$\cdot$	$-q_2$	$1 + q_2q_1$	r_2	$r_1 = r_2q_3 + r_3$
$\cdot$	$\cdot$	$\cdot$	$\cdot$	$\cdots\cdots$
$\cdot$	$\cdot$	$\cdot$	$\cdot$	$\cdots\cdots$
$\cdot$	α_{i-1}	β_{i-1}	r_{i-1}	$\cdots\cdots$
$-q_{i+1}$	α_i	β_i	r_i	$r_{i-1} = r_iq_{i+1} + r_{i+1}$
$\cdot$	$\alpha_{i-1} - q_{i+1}\alpha_i$	$\beta_{i-1} - q_{i+1}\beta_i$	r_{i+1}	$\cdots\cdots$
$\cdot$	$\cdot$	$\cdot$	$\cdot$	$\cdots\cdots$
$\cdot$	$\cdot$	$\cdot$	$\cdot$	$\cdots\cdots$
$\cdot$	$\cdot$	$\cdot$	r_n	$r_{n-1} = r_nq_{n+1} + d$
	α	β	d	$r_n = dq_{n+2} + 0$
			0	

Allora:

1. *La successione di numeri interi $a, b, r_1, r_2, \ldots, r_i, \ldots$ soddisfa alla condizione $0 \leq r_{i+1} < r_i$ (poiché r_{i+1} è il resto di una divisione intera per r_i), dunque* **termina necessariamente a 0**.

2. *In ogni riga della tabella risulta $r_j = \alpha_j\, a + \beta_j\, b$. Infatti ciò è vero per le prime due righe in tabella (quelle che competono ad a e b), e dunque supposta vera per le righe che competono a r_{i-1} e r_i dimostriamo che è vera per la riga che compete a r_{i+1}: infatti essendo $r_{i-1} = r_iq_{i+1} + r_{i+1}$, si ottiene*

$$r_{i+1} = r_{i-1} - r_iq_{i+1} = (\alpha_{i-1}a + \beta_{i-1}b) - q_{i+1}(\alpha_ia + \beta_ib) =$$
$$= (\alpha_{i-1} - q_{i+1}\alpha_i)a + (\beta_{i-1} - q_{i+1}\beta_i)b$$

che è quanto voluto. In particolare $\mathbf{d = \alpha\, a + \beta\, b}$.

3. *Si vede che* $d|r_n$ *(poiché il resto è 0), e dunque* $d|r_{n-1} = r_n q_{n+1} + d$. *Applicando iterativamente questo argomento all'eguaglianza* $r_{i-1} = r_i q_{i+1} + r_{i+1}$, *si deduce che* $d|r_j$ *per ogni* j, *e dunque anche* $d|a$ *e* $d|b$.

4. *Infine* $\mathbf{d} = (\mathbf{a}, \mathbf{b})$ *per il punto precedente e per il fatto che se* $d'|a$ *e* $d'|b$ *per* $d' \in \mathbb{Z}$, *allora anche* $d'|\alpha\, a + \beta\, b = d$.

Esempio 2.4. *Utilizzando l'Algoritmo di Euclide esteso calcoliamo il massimo comune divisore tra* 420 *e* 72, *ed esprimiamolo come loro combinazione intera.*

	$\vert$	1	0	$\vert$ 420	
-5	$\vert$	0	1	$\vert$ 72	$420 = 72 \cdot 5 + 60$
-1	$\vert$	1	-5	$\vert$ 60	$72 = 60 \cdot 1 + 12$
	$\vert$	-1	6	$\vert$ 12	$60 = 12 \cdot 5 + 0$
	$\vert$			$\vert$ 0	

Otteniamo dunque che $12 = (420, 72) = -1 \cdot 420 + 6 \cdot 72$.

ATTIVITÀ 2.5. *Si determinino* $d, \alpha, \beta \in \mathbb{Z}$ *tali che*

$$d = (24750, 3900) = \alpha \cdot 24750 + \beta \cdot 3900.$$

Concludiamo questa sezione lasciando ai più volonterosi un po' di lavoro per casa. Il primo di essi è rivolto a chi ha esperienza di programmazione:

HOMEWORK 2.6. *Si scriva il codice (ad esempio in PARI/Gp) per un algoritmo che, assegnati interi positivi* a *e* b, *calcoli il loro massimo comune divisore* $d = (a, b)$, *e determini* $\alpha, \beta \in \mathbb{Z}$ *tali che* $d = \alpha\, a + \beta\, b$.

Il secondo ha natura più teorica, ed è un risultato tanto elegante quanto importante:

HOMEWORK 2.7. *Si verifichi che gli interi che si ottengono come combinazione intera di preassegnati interi positivi* a, b *sono esattamente i multipli del loro massimo comune divisore* $d = (a, b)$, *cioè:*

$$\{z \in \mathbb{Z} \mid z = \alpha\, a + \beta\, b,\ \alpha, \beta \in \mathbb{Z}\} = d\mathbb{Z}.$$

3 Classi resto modulo n

In tutta questa sezione n denota un arbitrario, ma fissato, intero positivo.

Definizione 3.1. *Dati $a, b \in \mathbb{Z}$, diremo che essi sono tra loro* CONGRUI MODULO n*, e scriveremo*

$$a \equiv b \mod n$$

se essi differiscono per un multiplo di n, cioè se $n|a-b$.

Possiamo immaginare di disporre ordinatamente gli interi lungo un tragitto ad elica illimitata, in modo tale che essa si "avvolga sopra sè stessa" dopo aver dato posto esattamente ad n numeri interi consecutivi. In tal modo, scelto su di essa un qualunque intero a, "sopra" e "sotto" di a si troveranno esattamente tutti e soli gli altri interi che risultano congrui ad a modulo n.

Se $a \in \mathbb{Z}$, denoteremo con

$$\begin{aligned}\overline{a} &= \{a,\ a+n,\ a-n,\ a+2n,\ a-2n,\ a+3n,\ a-3n,\ \dots\} = \\ &= a + n\mathbb{Z} = \{b \in \mathbb{Z} \mid a \equiv b \mod n\}\end{aligned}$$

l'insieme di tutti gli interi congrui ad a modulo n.

Definizione 3.2. *Dati interi a, n, con $n > 0$, l'insieme*

$$\overline{a} = \{b \in \mathbb{Z} \mid a \equiv b \mod n\}$$

è detta CLASSE (RESTO) DI a MODULO n.

Con l'esperienza che ci è data nell'interpretare un orologio analogico, possiamo ad esempio affermare che, scelto $n = 12$,

$$3 \equiv 15 \mod 12;$$

ma è anche vero che

$$3 \equiv 15 \equiv 27 \equiv 39 \equiv \dots \mod 12$$

ed anche che

$$3 \equiv -9 \equiv -21 \equiv -33 \equiv \dots \mod 12.$$

È importante fin da subito osservare che **la proprietà** $a \equiv b \mod n$ **è equivalente all'eguaglianza** $\overline{a} = \overline{b}$ **tra classi modulo** n. Questo discende dal fatto che $n|a-b$ se e solo se $a-b \in n\mathbb{Z}$ se e solo se $a+n\mathbb{Z} = b+n\mathbb{Z}$. Ad esempio le congruenze sopra scritte sono del tutto equivalenti alla catena di equaglianze tra classi modulo 12

$$\overline{3} = \overline{15} = \overline{27} = \overline{39} = \cdots = \overline{-9} = \overline{-21} = \overline{-33} = \ldots$$

Osserviamo che ogni classe ha infiniti elementi, e che esistono solo n classi tra loro distinte: queste si possono scrivere, ad esempio, nella forma

$$\overline{0},\ \overline{1},\ \overline{2},\ \ldots,\ \overline{n-1}.$$

Notiamo che se $0 \leq a < n$, allora a coincide con il resto della divisione di un qualunque elemento della corrispondente classe $\overline{a}$ per n. Da qui il nome di **classe resto** modulo n.

Gli interi

$$0,\ 1,\ 2,\ \ldots,\ n-1$$

sono detti i RAPPRESENTANTI CANONICI delle classi resto modulo n.

Vale infatti il seguente risultato

Proposizione 3.3. *Dati $a, b, n \in \mathbb{Z}$, con $n > 0$, si ha che $a \equiv b \mod n$ se e solo se a e b hanno medesimo resto nella divisione per n.*

ATTIVITÀ 3.4. *Si dimostri la proposizione precedente.*