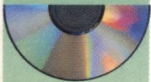


CampusPress Référence

Assembleur x86



Offert ! Un CD-ROM avec tous les exemples du livre, la version complète de l'assembleur Microsoft MASM 6.15, un éditeur de sources et une librairie de fonctions.

**Un ouvrage de référence
avec les jeux d'instructions
des derniers processeurs**



Kip Irvine

Réseaux
et télécom

Développement

Génie logiciel

Sécurité

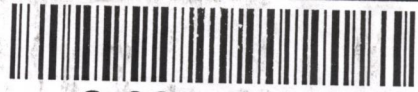
Système
d'exploitation


CampusPress

www.pearsoneducation.fr



2-005-659-1



2-005-659-1

Assembleur x86

Kip R. Irvine




CAMPUSPRESS

Table des matières

Introduction	1
Objectifs du livre	2
Connaissances préalables supposées	3
Structure du livre	3
Du Chapitre 1 au Chapitre 8	3
Du Chapitre 9 au Chapitre 17	4
Les annexes de référence	4
Les exemples du livre	5
Considérations techniques	5
Installation des logiciels	5
Génération des exécutables	6
Mises à jour	6
Remerciements	6
Chapitre 1. Concepts fondamentaux	7
Bienvenue dans le monde du langage assembleur	7
Les bonnes questions que vous devez vous poser	8
Applications en langage assembleur	14
Révision de section 01A	15
Le concept de machine virtuelle	15
L'histoire des assembleurs pour PC	19
Révision de section 01B	19
Représentation des données	20
Valeurs numériques binaires	21
Addition binaire	23
Format de stockage des valeurs binaires entières	24
Les valeurs entières hexadécimales	25
Valeurs entières signées	27
Stockage des caractères	30
Révision de section 01C	32

Opérations booléennes	34
Tables de vérité pour les fonctions booléennes	37
Révision de section 01D	38
Résumé	38
Chapitre 2. Architecture des processeurs IA-32	41
Concepts fondamentaux	41
Principe de la conception d'un micro-ordinateur	42
Cycle d'exécution d'instruction	44
Lecture depuis la mémoire	48
Fonctionnement d'un programme	49
Révision de section 02A	51
L'architecture des processeurs IA-32	52
Modes de fonctionnement	52
Environnement d'exécution de base	53
Petit historique des microprocesseurs Intel	57
Révision de section 02B	60
Gestion de la mémoire IA-32	60
Le mode réel	61
Le mode protégé	63
Révision de section 02C	66
Les composants d'un micro-ordinateur IA-32	66
La carte mère	66
Sous-système d'affichage vidéo	69
Les différents types de mémoires	69
Les ports d'entrées/sorties	70
Révision de section 02D	72
Le mécanisme d'entrées/sorties	72
Les différentes couches d'entrées/sorties	72
Révision de section 02E	75
Résumé	76
Chapitre 3. Principes du langage assembleur	79
Éléments constitutifs du langage assembleur	79
Constantes entières	80
Expressions entières	81
Constantes de nombres réels	82
Constantes caractères	82
Constantes chaînes	83

Mots réservés du langage	83
Identificateurs	83
Directives	84
Instructions	85
Commentaires	88
Révision de section 03A	88
Premier exemple : addition de trois nombres entiers	89
Listing source du programme	89
Résultats affichés	89
Commentaires détaillés du programme source	90
Modèle de programme source	93
Révision de section 03B	94
Assemblage, liaison et exécution d'un programme	94
Le cycle assemblage-liaison-exécution	95
Révision de section 03C	98
Définition/déclaration des données	99
Types de données intrinsèques	99
Instructions de déclaration de données	99
Définition de données BYTE et SBYTE	100
Déclarations de données WORD et SWORD	103
Déclarations de données DWORD et SDWORD	104
Déclarations de données QWORD	104
Déclarations de données TBYTE	105
Déclarations de données non entières (réels)	105
Ordre de stockage des bits (ordre "little endian")	106
Ajout de variables au programme AddSub	106
Déclaration de données non initialisées	107
Révision de section 03D	108
Constantes symboliques	108
Directive égalité (=)	109
Calcul de la taille des tableaux et des chaînes	110
Directive EQU	111
Directive TEXTEQU	113
Révision de section 03E	113
Programmation en mode réel (facultatif)	114
Principales modifications	114
Résumé	115
Exercices de programmation	117
Résumé	119
Exercices de programmation	120

Chapitre 4. Transferts de données, adressage et arithmétique	123
Instructions de déplacement de données	123
Types formels d'opérandes	124
Opérandes mémoire directs	124
Instruction de déplacement <i>MOV</i>	125
Gestion du zéro et de l'extension de signe des entiers	127
Instructions <i>LAHF</i> et <i>SAHF</i>	129
Instruction <i>XCHG</i>	129
Ajout d'un décalage direct à un opérande	130
Programme d'exemple (Moves.asm)	131
Révision de section 04A	132
Addition et soustraction	133
Instructions <i>INC</i> et <i>DEC</i>	133
Instruction <i>ADD</i>	134
Instruction de soustraction <i>SUB</i>	134
Instruction de négation <i>NEG</i>	135
Ecriture d'expressions arithmétiques	135
Drapeaux affectés par les opérations arithmétiques	136
Programme d'addition d'exemple (AddSub3)	139
Révision de section 04B	141
Opérateurs et directives relatifs aux données	141
L'opérateur <i>OFFSET</i>	142
La directive <i>ALIGN</i>	143
L'opérateur <i>PTR</i>	143
L'opérateur <i>TYPE</i>	145
L'opérateur <i>LENGTHOF</i>	145
L'opérateur <i>SIZEOF</i>	146
La directive <i>LABEL</i>	146
Révision de section 04C	147
Adressage indirect	147
Opérandes indirects	148
Les tableaux (array)	149
Opérandes indexés	150
Pointeurs	152
Révision de section 04D	154
Les instructions de boucles <i>JMP</i> et <i>LOOP</i>	154
L'instruction de saut incondtionnel <i>JMP</i>	155
L'instruction de boucle <i>LOOP</i>	155
Calcul de la somme d'un tableau d'entiers	157

Copie d'une chaîne	158
Révision de section 04E	159
Résumé	160
Exercices de programmation	161
Chapitre 5. Procédures	165
Introduction	165
Liaison avec une librairie externe	165
Informations préliminaires	166
Révision de section 05A	168
La librairie Irvine32.lib	168
Présentation	168
Présentation individuelle des procédures	170
Le fichier Irvine32.inc	176
Programme de test de la librairie Irvine32	178
Révision de section 05B	181
Opérations liées à la pile (<i>stack</i>)	182
Pile d'exécution	182
Instructions <i>PUSH</i> et <i>POP</i>	184
Révision de section 05C	188
Définition et utilisation des procédures	188
Directive <i>PROC</i>	188
Exemple d'addition des entiers d'un tableau	195
Organigrammes fonctionnels (<i>flowchart</i>)	196
Sauvegarde et restauration des registres	197
Révision de section 05D	199
Modularisation des programmes par les procédures	199
Conception d'un programme d'addition d'entiers	200
Révision de section 05E	205
Résumé	205
Exercices de programmation	207
Chapitre 6. Traitements conditionnels	209
Introduction	209
Instructions booléennes et comparaisons	210
Les drapeaux du processeur	211
Instruction ET logique (<i>AND</i>)	211
Instruction OU logique (<i>OR</i>)	212
Instruction OU exclusif (<i>XOR</i>)	214

Instruction d'inversion <i>NOT</i>	215
Instruction <i>TEST</i>	216
Instruction <i>CMP</i>	216
Armement/désarmement des drapeaux individuels	218
Révision de section 06A	218
Sauts conditionnels	219
Gamme d'instructions <i>Jcondition</i>	220
Présentation des instructions de saut conditionnel	221
Exemples d'utilisation des sauts conditionnels	223
Instructions de test de bits	228
Révision de section 06B	230
Instructions de boucle conditionnelle	231
Instructions <i>LOOPZ</i> et <i>LOOPE</i>	231
Instructions <i>LOOPNZ</i> et <i>LOOPNE</i>	231
Révision de section 06C	232
Structures conditionnelles	232
Instruction <i>IF</i> avec bloc d'instructions	233
Expressions composées	235
Boucles <i>WHILE</i>	236
Branchements multiples pilotés au moyen d'une table	237
Révision de section 06D	241
Une application concrète : la machine à états finis	241
Validation de la saisie d'une chaîne	242
Validation de la saisie d'un entier signé	243
Les MEF et l'assembleur	243
Révision de section 06E	247
La directive conditionnelle <i>.IF</i>	247
Comparaisons signées et non signées	249
Expressions composées	250
Directives <i>.REPEAT</i> et <i>.WHILE</i>	252
Résumé	254
Exercices de programmation	255
Chapitre 7. Arithmétique des entiers	259
Introduction	259
Instructions de décalage et de rotation de bits	260
Instruction <i>SHR</i> (SHift Right)	262
Instructions <i>SAL</i> et <i>SAR</i> (décalages arithmétiques)	263
Instruction <i>ROL</i>	263

Instruction <i>ROR</i>	264
Instruction <i>RCL</i>	264
Instruction <i>RCR</i>	265
Instructions <i>SHLD/SHRD</i>	266
Révision de section 07A	267
Applications pratiques des décalages et des rotations	268
Décalage de plusieurs doubles-mots	268
Multiplication binaire	268
Affichage des bits individuels	269
Isolation d'un champ de bits	270
Révision de section 07B	271
Instructions de multiplication et de division	271
Instruction <i>MUL</i>	272
Instruction <i>IMUL</i>	273
Instruction <i>DIV</i>	274
Divisions entières signées	276
Complément au sujet des expressions arithmétiques	278
Révision de section 07C	280
Additions et soustractions étendues	281
Instruction <i>ADC</i>	281
Exemple complet d'addition étendue	281
Instruction <i>SBB</i>	283
Révision de section 07D	283
Arithmétique décimale compactée et ASCII	284
Instruction d'addition <i>AAA</i>	285
Instruction de soustraction <i>AAS</i>	285
Instruction de multiplication <i>AAM</i>	286
Instruction de division <i>AAD</i>	286
Entiers décimaux compactés	286
Résumé	287
Exercices de programmation	288
Chapitre 8. Procédures (niveau 2)	291
Introduction	291
Variables locales	292
Directive <i>LOCAL</i>	293
Révision de section 08A	295
Paramètres de pile	295
Directive <i>INVOKE</i>	296

Directive <i>PROC</i>	299
Directive <i>PROTO</i>	300
Passage des paramètres par valeur ou par référence	302
Catégories de paramètres	303
Exemple : permutation de deux entiers	304
Conseils de débogage	305
Révision de section 08B	307
Cadre de pile	308
Modèle mémoire	309
Spécificateurs de langage	310
Accès explicites aux paramètres de pile	312
Passage de paramètres par référence	314
Création de variables locales	316
Instructions <i>ENTER</i> et <i>LEAVE</i>	317
Révision de section 08C	319
Récursivité	319
Calcul d'une somme par récursivité	321
Exemple de calcul d'une factorielle	322
Révision de section 08D	324
Création d'un programme multifichier	325
Révision de section 08E	332
Résumé	332
Exercices de programmation	334
Chapitre 9. Chaînes et tableaux	335
Introduction	335
Instructions Intel de traitement de chaînes	336
<i>MOVSB</i> , <i>MOVSW</i> et <i>MOVSD</i>	338
<i>CMPSB</i> , <i>CMPSW</i> et <i>CMPSD</i>	339
<i>SCASB</i> , <i>SCASW</i> et <i>SCASD</i>	342
<i>STOSB</i> , <i>STOSW</i> et <i>STOSD</i>	342
<i>LODSB</i> , <i>LODSW</i> et <i>LODSD</i>	343
Révision de section 09A	344
Procédures de traitement de chaînes de Irvine32	344
Str_compare	344
Str_length	346
Str_copy	346
Str_trim	347

Str_ucase	349
Révision de section 09B	349
Tableaux à deux dimensions	350
Opérandes base-index	350
Opérandes base-index-déplacement	352
Révision de section 09C	353
Recherche et tri de tableaux d'entiers	353
Tri par paires de type Bubble	354
Techniques de recherche binaire	356
Révision de section 09D	364
Résumé	364
Exercices de programmation	365
Chapitre 10. Structures de données et macros	369
Structures	369
Structure <i>COORD</i>	370
Définition d'une structure de données	370
Déclaration des variables structures	371
Références aux variables structures	372
Affichage de l'heure système	374
Imbrication de structures de données	378
Exemple de l'homme titubant	378
Les unions	382
Révision de section 10A	384
Macros	384
Présentation	384
Définition d'une macro	385
Etude de macros prédéfinies	388
Macros imbriquées	392
Exemple complet : Wraps.asm	393
Révision de section 10B	395
Directives d'assemblage conditionnel	395
Test de présence des paramètres	396
Valeur par défaut des paramètres	397
Expressions booléennes	398
Directives <i>IF</i> , <i>ELSE</i> et <i>ENDIF</i>	398
Directives <i>IFIDN</i> et <i>IFIDNI</i>	399
Opérateurs spéciaux	400
Fonctions macros	406

Révision de section 10C	408
Directives de bloc de répétition	409
Directive <i>WHILE</i>	410
Directive <i>REPEAT</i>	410
Directive <i>FOR</i>	411
Directive <i>FORC</i>	412
Exemple de gestion d'une liste liée	412
Révision de section 10D	414
Résumé	415
Exercices de programmation	416
Chapitre 11. Programmation Windows 32 bits	419
Programmation pour la console Win32	419
Principes élémentaires	421
Fonctions de la console Win32	424
Opérations d'entrée de console	428
Opération de sortie de console	431
Fonctions de lecture et d'écriture dans les fichiers	434
Manipulation de la fenêtre de console	440
Contrôle du curseur	444
Contrôle de la couleur du texte	445
Fonctions de date et d'heure	447
Révision de section 11A	453
Conception d'une application graphique Windows	454
Structures de données requises	455
Fonction <i>MessageBox</i>	457
Procédure principale <i>WinMain</i>	457
Procédure de traitement des messages <i>WinProc</i>	458
Procédure de gestion d'erreur <i>ErrorHandler</i>	458
Listing complet du programme	459
Révision de section 11B	464
Gestion mémoire des processeurs IA-32	464
Adresses linéaires	465
Translation des pages	470
Révision de section 11C	472
Résumé	473
Exercices de programmation	474

Chapitre 12. Interface avec les langages de haut niveau	477
Introduction	477
Conventions d'interface	477
Révision de section 12A	479
Code assembleur en ligne	480
La directive <code>__asm</code> de Microsoft Visual C++	480
La directive <code>__asm</code>	480
Exemple de cryptage de fichier	483
Révision de section 12B	486
Liaison de l'assembleur à un programme C++	487
Liaison avec un programme Borland C++	488
Un exemple de lecture directe de disque	490
Un second exemple : génération de grands entiers	495
L'assembleur pour optimiser du code C++	497
Révision de section 12C	504
Résumé	504
Exercices de programmation	505
Chapitre 13. Programmation MS-DOS 16 bits	507
Le système MS-DOS et le PC IBM	507
Cartographie mémoire en mode réel	508
Redirection des entrées/sorties	510
Interruptions logicielles	511
L'instruction <code>INT</code>	511
Révision de section 13A	513
Appels de fonctions MS-DOS (<code>INT 21h</code>)	513
Echantillon de fonctions de sortie (d'affichage)	515
Exemple avec le programme Hello World	518
Un florilège de fonctions d'entrée	519
Fonctions de date et d'heure	523
Révision de section 13B	527
Fonctions d'entrée/sortie fichier standard de MS-DOS	528
Fonction de libération de handle fichier (<code>3Eh</code>)	531
Fonction de déplacement du pointeur fichier (<code>42h</code>)	532
Fonction de récupération de la date et de l'heure de création d'un fichier (<code>5706h</code>)	532
Deux routines de la librairie de l'auteur	533
Exemple complet : lecture et copie d'un fichier texte	534
Exemple de lecture de la queue de ligne de commande MS-DOS	537
Exemple de création d'un fichier binaire	539

Révision de section 13C	542
Résumé	543
Exercices de programmation	545
Chapitre 14. Concepts de base des disques	547
Systèmes de stockage sur disque	547
Pistes, cylindres et secteurs	548
Volumes de disque ou partitions	550
Révision de section 14A	552
Systèmes de fichiers	552
Le système FAT12	554
Le système FAT16	554
Le système FAT32	555
Le système NTFS	555
Zones primaires	556
Révision de section 14B	558
Structure arborescente des disques	558
Structure des répertoires sous MS-DOS	559
Les noms de fichier longs sous MS-Windows	562
Table d'allocation des fichiers (FAT)	564
Révision de section 14C	565
Lecture et écriture directe de secteurs disque (7305h)	566
Exemple d'affichage du contenu d'un secteur	567
Révision de section 14D	572
Fonctions fichiers au niveau système	572
Obtention de l'espace disque libre (7303h)	573
Création d'un sous-répertoire (fonction 39h)	576
Suppression de sous-répertoire (fonction 3Ah)	577
Sélection du répertoire courant (fonction 3Bh)	577
Nom du répertoire courant (fonction 47h)	577
Révision de section 14E	578
Résumé	578
Exercices de programmation	579
Chapitre 15. Programmation au niveau BIOS	583
Introduction	583
Zone de données du BIOS (data area)	584
Saisies clavier par INT 16h	585
Fonctionnement du clavier	586

Fonctions de la famille INT 16h	587
Révision de section 15A	593
Programmation VIDEO avec INT 10h	594
Principes de base	594
Contrôle de la couleur d'affichage	596
Les fonctions vidéo INT 10h	598
Exemple de procédures de la librairie de l'auteur	611
Révision de section 15B	612
Affichages graphiques avec INT 10h	613
Fonctions graphiques de INT 10h	613
Exemple de tracé de ligne	615
Coordonnées cartésiennes	617
Conversion de coordonnées cartésiennes en coordonnées écran	619
Révision de section 15C	620
Accès graphiques vidéo directs	621
Le mode 13h : 320 × 200 en 256 couleurs	621
Exemple d'écriture directe en mémoire vidéo	623
Révision de section 15D	626
Programmation de la souris	626
Les fonctions INT 33h dédiées à la souris	627
Révision de section 15E	638
Résumé	639
Exercices de programmation	640
Chapitre 16. Programmation MS-DOS pour experts	643
Introduction	643
Définition explicite des segments	644
Directives de segmentation simplifiées	644
Définition explicite des segments	647
Redéfinition de segment (override)	651
Combinaison de segments	651
Révision de section 16A	653
Implantation mémoire d'un programme en cours d'exécution	654
La zone PSP	655
Structure des programmes .COM	655
Structure d'un programme .EXE	657
Révision de section 16B	659
Gestion des interruptions	659
Interruptions matérielles	661

Instructions de contrôle des interruptions	663
Conception d'un gestionnaire d'interruptions	664
Programmes résidents	667
Application : le programme No_Reset	668
Révision de section 16C	672
Résumé	673
Annexe A. Installation et utilisation de MASM	675
Installation du CD-ROM	675
Assemblage et liaison de programmes 32 bits en mode protégé	676
Débogage en mode protégé	677
Le fichier de commandes make32.bat	677
Assemblage et liaison de programmes 16 bits en mode réel	678
Le fichier de commandes make16.bat	679
Débogage en mode réel	679
Annexe B. Le jeu d'instructions Intel	681
Introduction	681
Drapeaux (flags)	681
Descriptions et formats des instructions	682
Le jeu d'instructions	683
Annexe C. Interruptions BIOS et MS-DOS	719
Introduction	719
Interruptions PC	720
Fonctions des services MS-DOS (INT 21h)	723
Fonctions BIOS vidéo (INT 10h)	729
Fonctions BIOS clavier (INT 16h)	731
Fonctions souris (INT 33h)	732
Annexe D. Référence de MASM	733
Introduction	733
Notation de la syntaxe	734
Mots réservés du langage de MASM	734
Noms officiels des registres	735
Microsoft Assembler (ML)	735
Le lieur LINK	738
Options	738
Le débogueur CodeView	741
Directives MASM	742

Symboles de MASM	762
Opérateurs de MASM	765
Opérateurs d'exécution de MASM	770
Annexe E. Réponses aux questions des révisions de sections	773
Introduction	773
Index	803